Classification Management

JOURNAL OF THE NATIONAL
CLASSIFICATION MANAGEMENT SOCIETY

VOLUME V No. 2 - 1969

Classification Management

JOURNAL OF THE NATIONAL
CLASSIFICATION MANAGEMENT SOCIETY

VOLUME V No. 2 - 1969

CONTENTS

PAPERS FROM THE FIFTH NATIONAL SEMINAR

Published semiannually. Views expressed by individuals herein do not necessarily represent views of NCMS or of the individuals' employers.

PAPERS FROM THE FIFTH ANNUAL SEMINAR NATIONAL CLASSIFICATION MANAGEMENT SOCIETY

Washington, D.C.

July 22-24, 1969

MILITARY AND INDUSTRIAL COMPLEXITIES

Alfred B. Berry, President, American Society for Industrial Security

I am most pleased to have been invited to your fifth annual seminar and to address members of the National Classification Management Society. On behalf of the American Society for Industrial Security, I want to congratulate your seminar committee for their efforts in making this seminar an accomplished fact.

Prior to coming here, I looked through your journals containing the proceedings for your last three seminars and re-read several of the presentations and subsequent discussions. A profound discovery was made! It isn't the "military-industrial complex" with which we need concern ourselves but rather the *military-industrial complexities!* And the membership of NCMS is to be commended for having concerned themselves with so many of these problems.

Striving toward an analytical approach for specific security problems is a primary objective for both NCMS and ASIS. Many of you have witnessed the transitional phases of the industrial security program and will recall the 14-page pamphlet issued by the Munitions Board. If you still have a copy in file, compare it with the 236-page Department of Defense Industrial Security Manual which we now have.

Today, not many people realize how fast technology is advancing. To illustrate this point, if we consider the history of man composed of life spans of men, we are talking about approximately 800 men. The last 650 of these men lived in caves. Only the last 8 had seen a printed word; only the last 4 could measure heat or cold with any degree of accuracy; only the last 3 could measure time with any accuracy; only the last 2 have used an electric motor, and everything else that you see around you today was developed during the lifespan of the last or 800th man. Furthermore, our knowledge is doubling every 8 to 10 years and 10 years from now we will know as much as what has taken our ancestors the last 50,000 years to learn. The learning curve is going straight up which means greater exposure, greater problems, and making it increasingly important and necessary that we take prompt action to protect both department of defense classified and proprietary information.

It is obvious to all of us that our

security responsibilities are also on the up-swing with increasing demands placed upon our ability to assess a myriad of security functions and evaluate them in relation to cost effectiveness. Management expects *us* to have the answers. We must be analytical to be responsive. We must identify and anticipate problems and take the necessary preventive steps before they occur.

I am gratified by observing the dedicated security professionals of NCMS who are devoting their time and efforts in attending this seminar and participating in the exchange of information and ideas. Your selection of distinguished speakers from the Congress, military establishment, industry, and two gentlemen whom we may identify as scholars is indicative of the seriousness and professional atmosphere which you have brought to this seminar.

During a recent meeting of the ASIS Classification Management Committee, it was the consensus of the Committee that interface with NCMS should be direct and continuing. Providing for a cooperative exchange of information and research data should be beneficial for both societies. In furtherance of this effort, I should like to invite the membership of NCMS to submit articles for publication in our ASIS magazine. The ASIS magazine is published bi-monthly and professional security articles are always most welcome. Mr. Bill Wright, our ASIS executive director in Washington, advises that we could assist in facilitating the availability of reprints by a waiver of copyrights and providing reproducible proofs to NCMS.

Classification Management is indeed the bedrock foundation upon which our industry security program is built and it is well that a society, such as your own, has emerged devoting itself exclusively to this business. While Classification Management would appear to be a singular element of industrial security, we who are actively engaged in this profession realize and appreciate the fact that all Department of Defense security requirements are predicated on the many and varied considerations applicable to the protection of classified Defense Information.

Classification Management is therefore most deserving of special attention. Giving serious consideration to the basic criteria for classifying and declassifying defense information can very well provide significant contributions to your firm's cost effectiveness programs.

Many of you who have engaged in cost effectiveness surveys have perhaps attempted to determine the actual cost for maintaining strict accountability for a single secret document during the course of a year. Regardless of the figures which you may have come up with, we are all in agreement on one thing—it does cost money!

I am sure that you have also considered many other derivative cost ramifications attributed to the protection and safeguarding of classified information such as secret, top secret, special access programs and closed and restricted area controls.

Disseminating accurate and definitive classification guidance and providing for prompt downgrading and declassification of information are considerations of paramount import-

ance both to the Department of Defense and industry.

Some time ago, my office initiated a letter to Mr. George MacClain suggesting that the automatic, time-phased downgrading and declassification system be revamped providing for two group marking notations replacing the four that we now have. The basic idea was to simplify downgrading by having one group which was excluded from downgrading and declassification and designating a group to replace the present Groups 3 and 4 which would provide for both downgrading and declassification on a definite time-phased basis. This, of course, would eliminate present problems in differentiating between the present Group 3 and Group 4 marking notations and effecting realistic declassification of information. It is my understanding that the automatic, time-phased downgrading and declassification system is being revised by DOD and should rectify many of our current problems in this area.

It has been my experience that our counterparts in the Department of Defense have been most receptive and appreciative of analyses and suggestions submitted by industry. Their interest and active participation in the "give and take" discussions which ensue in seminars such as this is indicative of the fine relationship existing between professional government security men and those of us in industry. And, as we have often remarked, we are both working toward the same goal.

No one has a special lease on ideas. And I am certain that many of you have some fine ones to share with your associates in industry. I would suggest also that the results of such efforts rendered in surveys and analyses should be formalized and submitted to DOD. This is not to say that you should expect all of your pet projects to be sanctioned and adopted by DOD but perhaps some of them will. In any event, I do know that the government is appreciative of such efforts.

Many of you most probably received copies of the NSIA proposal concerning suggested ISM procedural changes for classified document retention. This is, of course, with reference to Paragraphs 5K and 5L which we all referred to for a number of years as 5J and 5K. The interpretation of this requirement has involved numerous discussions between industry and government over the years. While I do not know what position NCMS may have adopted concerning this subject, I thought that the substance of my response to both AIA and EIA concerning the NSIA proposal could be of some interest.

The NSIA proposal, accepted as codsia Case 33-9, is, I believe, a step in the right direction. However, I personally feel that it falls somewhat short of suggesting a solution to the basic problem concerning retention of classified documents by defense contractors. Going through the formalized routine of requesting authorization for retention of classified documents is no small task. The following points are suggested as major items for consideration:

1. The Department of Defense (i.e. the Army, Navy and Air Force) is continually indicating a desire that major defense contractors be cognizant of advanced technology

or advances in the "state of the art."

We need only point to the thousands of documents distributed to contractors by the Defense Documentation Center and the Technical Objectives Documents (TOD) program.

2. So long as we remain in the defense business and retain our facility clearance, we should only be required to *reduce to an absolute minimum the classified material on hand upon contract termination or in any of the other situations.*

Approval should not be required for the contractor to retain a limited number of all classified documents generated unless strictly prohibited by the contracting officer in special situations.

3. The contractor's cognizant security office, in performing its primary responsibility of inspecting contractor facilities, is in an excellent position to ensure that only a minimum number of classified documents are retained upon contract termination. In those situations where a contractor is not actively engaged in classified defense work or cannot justify continued cognizance of advanced technology, all classified documents generated should be returned to the contracting officer or destroyed.

The foregoing arguments admittedly are not new. But the basic contention is one which I feel is worthy of consideration (i.e. that there is no need for formally requesting retention authorization when continued possession of classified documents is an obvious, common sense requirement which can be monitored quite easily by the cognizant security office). There has never been any argument with the basic DOD philosophy stated in paragraph 19.a. of the ISM which states:

> "The contractor shall establish a program for the review of classified material for the purpose of reducing to an absolute minimum the quantity on hand at any given time."

The foregoing is not intended as a "position paper" dealing with the problem in its entirety but merely contains the substance of my response to the NSIA proposal. It is something which NCMS might want to pursue since it is a current item.

Another thought which I should like to present to you in passing was originated by the Industrial Security Subcommittee of EIA suggesting industry/government collaboration on a re-write of the ISM. I personally feel that the idea has considerable merit.

Cognizant security office field inspectors, during the course of conducting recurrent "696" inspections, have the opportunity of considering the written ISM requirement and reviewing the contractor's procedural application. They sometimes reflect that a particular contractor's interpretation of an ISM requirement and his innovations and methodology in drafting certain procedural instructions would be very worthwhile for other contractors to consider.

To improve government/industrial security programs, there must first of all be an established method to insure that all programs, regulations and problems are thoroughly analyzed. This is a very difficult and time-consuming task for the Office of Industrial Security, DSA to perform.

One solution which might lessen the problem would be to give serious consideration to soliciting industry/government collaboration on a rewrite of the ISM. This would provide the government with statistical data and detailed information, gathered from experienced industrial security management, which would have a direct bearing on the applicability of specific regulations and improve the overall effectiveness of the ISM.

In this manner, analytical and factual data would flow upward and all ramifications of a problem considered before a decision is handed down. Cognizant security offices should be the focal points in conducting nation-wide surveys. Contractors' responses to queries should be forwarded with cognizant security office comments to Headquarters, Office of Industrial Security, DSA. Such surveys and responses thereto would provide the basic criteria for ISM and DODISR revisions. While good security can never be a static thing, an annual revision of the ISM should not be necessary.

Initially, however, and perhaps coincident with or prior to the next major revision of the ISM, a program could be initiated to obtain industry's participation in a complete rewrite of the manual. Many have voiced opinions regarding general considerations such as format, organization of material, utilization of footnotes, restructuring of the indices, and a revamping of sections and page numbering sequence to facilitate the insertion of subsequent revisions. As mentioned previously, the collection of statistical data and giving consideration to contractors' innovations and methodology could provide the basis for updating specific security regulations.

I do want to convey a few of the recent accomplishments of ASIS and relate to you some specific items concerning imminent objectives.

During the month of February, letters were sent to all members of Congress recommending that certain principles be incorporated as essential tenets in any forthcoming security legislation. While we neither endorsed nor disavowed any particular resolution concerned with the industrial security program, our society is at least becoming vocal.

Several manuals are being prepared, specifically: *safeguarding classified information, security investigations, protection of proprietary information* and *physical security.* When prepared, these will be published in the *"Industrial Security"* magazine in such a manner (i.e. center inserts) to facilitate re-printing.

Our *"Industrial Security"* magazine was first published on a twice yearly basis in 1957. It then grew into a quarterly and now, of course, is a bimonthly publication.

To make our magazine available as reference and source material, all back issues have been microfilmed and provided to various educational institutions. This has been accomplished by our ASIS foundation. Together with the microfilmed back issues, these institutions will receive lifetime subscriptions to our magazine. Total cost for this service is $50.

The ASIS foundation was incorporated as a separate legal entity in October of 1966 devoting itself exclusively to educational and immed-

iately related functions.

Serious efforts have been directed toward reviewing and promoting industrial security curricula to be taught at institutions of higher education.

During the month of February, the University of Southern California's graduate school of business administration offered and successfully presented "Industrial Security" as an executive program. The program was undertaken in cooperation with representatives of the American Society for Industrial Security.

The Lawrence Radiation Laboratory of the University of California is continuing with its efforts in providing a security summer study group. The curriculum has received favorable comment from Northeastern University and will evidently influence implementation of additional courses of study there.

As you can see, ASIS members are actively participating in promoting our Society's objectives and striving toward professionalism in security.

Thinking of the effort required for active participation in both your Society and mine as well as the work involved in presenting worthwhile seminars reminds me of the final lines of a melodrama which I saw several years ago—I don't know how many! The movie was titled "The Shrike" with June Allyson and Jose Ferrer starring. The "now generation" could perhaps benefit by giving a little thought to such a basic, realistic formula. It went something like this: "I've learned one thing . . . happiness doesn't come easily . . . one has to work at it!"

Whether striving toward a particular goal, or success, or happiness, it is certain that we *do* have to work at it.

In closing, I would like to remind those of you who are members of ASIS of our forthcoming 15th Annual Seminar to be held in Washington, D.C. during September 16th through September 18th. Those of you who are not members are, of course, equally welcome. I hope to see you there. Thank you.

KEYNOTE ADDRESS

Colonel Andrew A. Aines, Chairman

Committee on Scientific and Technical Information, Federal Council for Science and Technology

It is a fairly accurate observation, I believe, that the most fashionable way to present a speech today is to describe a *problem* which turns out to be grave, challenging, complex and virtually impossible to solve. How the problem is presented depends on the speaker's personality and involvement. He can depict it in a variety of ways, ranging from lurid, colorful and explosive, to calm, detached and moderate and anything in between these two poles. After the problem has been presented and the speaker hopefully has the full and unqualified attention of the audience, he then proceeds to reveal in reassuring terms just what he or others are doing to beat the problem into submission. This is the time-proven formula, and I see no need to completely rewrite the script, although I may take some liberties from time to time, and even agree in advance that some of my remedies are probably no better than those of any other witch doctor or overworked bureaucrat.

While the theme of this conference involves information, classification, and freedom, I think it appropriate at the outset to use instruments that more accurately describe what is going on than we can using our own rather primitive sensory equipment. If we were able to devise a social barometer or thermometer, we would probably record the following.

Society is in a state of flux. Anxiety is the best keyword, perhaps, that describes this era. We are in a trough of despair as we watch our treasured institutions totter under the attack of extremists. In the midst of an unparalleled prosperity in our country, we find turmoil and challenge and disaffection. Conflict is seen everywhere we turn: in our cities, between races, in universities, between age groups, and between authorities and dissidents. The thermometer would show dangerously high temperatures; the barometer, increasing pressures.

Loren Eiseley sees the society "secretly homesick for a lost world of inward tranquility." In a book that will soon be on the market, *The Unexpected Universe,* Eiseley writes about elements in our country and elsewhere which have deliberately taken the road which abandons the gains of the past along with hard-won conceptual tools and values. He writes: "The lessons of the past have been found to be a reasonably secure instruction for proceeding against the unknown future. To hurl oneself recklessly, without method, upon a future that we ourselves have complicated is a sheer nihilistic rejection of all that history, including the classical world, can teach us."

It is extraordinary behavior to the "over thirties," as we are contemptuously characterized, to watch ideals trampled in the name of higher ideals, which are rarely if at all described.

But I think it would be wrong to mistake the symptoms for the disease itself. That many bright and competent people are being driven to excesses by their own particular Furies should give cause to more than passing concern.

Now, I do not want to spend any time talking about the obvious. Every one in this room is just as familiar as I am with the data brought into our homes and offices disclosing the disequilibrium around us. The point should be made however that management of classification of knowledge must take into consideration the extraordinary skewing and shifting that is evident in the world we live in. None of us can operate in a vacuum; we cohabit a very real world, and if we are to successfully adapt to the ever-changing conditions, we simply have to comprehend the present and reasonably predict the near future, at least.

For example, we seem to be shifting from what has been referred to as a Cartesian view of the future in which the focus has been on parts and elements, to a configuration view, where the emphasis turns out to be instead on wholes and patterns, on the gestalt. Peter Drucker has written about this and so has Marshall McLuhan. The latter has created a new cult, as it were, which carries its counterpart of Mao's little red book with his collected sayings. I will have a few comments about McLuhan shortly, but I want to sharpen your thoughts about the meaning attached to shifting Cartesian thought away from the center ring.

If these observers are correct, we are beginning to discard the linear approach towards working and thinking, where event faithfully follows cause and specific reactions inevitably follow specific actions. McLuhan talks about "all-at-onceness," pointing out that a civilization that receives its knowledge by the electric media, TV, radio, etc., will not be the same as one that obtains, stores and uses its knowledge bank, based on the ink-print or Gutenberg medium, to use some of the newer jargon.

The most probable assumption, if you will accept their views, is that all of the old disciplines, demarcations, and even some institutions based on the old way of thinking and doing, will crumble and become obsolete with the passage of time. For many centuries, knowledge and action had little to do with each other. Technology until the second half of the 19th century was separate from science. Today, according to Drucker, both are drawn together; moreover the search for knowledge, the organization of knowledge, have gravitated around the areas of application rather than around the subject areas of the disciplines.

In his book, *The Age of Discontinuity,* Drucker points out that:

"This is a symptom of the shift in the meaning of knowledge from an end in itself to a resource, that is, a means to some result. What used to be knowledge is becoming information. What used to be technology is becoming knowledge. Knowledge as the central energy of modern society exists altogether in application and when it is put to work. Work, however, cannot be

defined in terms of disciplines. End results are interdisciplinary out of necessity."

What does it mean to recognize that research produces information rather than knowledge? For one thing, it becomes necessary to organize both the handling and the application of information to end results. Information left in vaults or files or libraries cannot be considered useful or legitimate. It is in this sense that the comment of the former president, Lyndon B. Johnson, made when he signed the State Technical Services Act, September 1965, becomes important. He said:

". . . the test of our generation will not be the accumulation of knowledge. In that we have surpassed all the ages of mankind combined. Our test will be how well we apply that knowledge for the betterment of mankind."

More recently, Dr. Lee A. DuBridge, the President's Science Adviser stated in *Science* (11 August 1967):

"If the world's troubles seem tragic and complex, this is not because we have too much knowledge, but because we have not learned how to use all our knowledge effectively."

Even more recently, President Nixon stated in the International Electronic and Aerospace Report, Oct/Nov 1968:

"The essence of preventing duplication of effort, and the consequent waste of money, lies in rapid dissemination of information throughout the world . . . Our government . . . should set up regular procedures for widespread exchange with other countries."

I think that it is important that we understand the changing attitude towards information in so many quarters. The need for *utilization* of knowedge is taking on new dimensions. It is inevitable that application of knowledge take its rightful place beside generation, storage, dissemination and protection of information.

In effect, it becomes necessary to you ladies and gentlemen whose lives are dedicated to the most necessary task of protecting information and data vital to the interests of our country to consider your roles against this background. It could very well be true that you are powerless to do more than safeguard information entrusted to your care, but you must also consider yourselves part of the community that handles knowledge to obtain maximum benefits for the people of the United States and the world. I cannot help but think that it makes a difference. You are much more than lonely custodians of information, selected information, as I view your function.

On the other hand, there has to be truth in something that Marshall McLuhan said in his *Medium is the Message*. He said that "real total war has become information war . . . being fought by subtle electric informational media — under cold conditions, and constantly." This statement will provide you with some amusement, I would presume, because you have fully understood that fact of life long before it took the form of a profound dictum by McLuhan. But I think it would be incorrect, if we simply

thought that he was referring to the so-called cold war and the protection of information necessary for our security. His concern is with the involvement that electric circuitry brings to mankind. He argues: "Information pours upon us, instantaneously and continuously. As soon as information is acquired, it is very rapidly replaced by still newer information."

About this point, you might want to ask a question like — McLuhan may be correct when he talks about all information, but our concern is more limited to a specific kind of information, so why should we worry about electric information and all of that jazz?

It is a good and logical question, but I think it would be short-sighted on our part if we did not recognize that scientific and technical information, especially the products of our huge United States research and development programs, is destined for electronic information networks, networks that are already in the early stages of development.

The Committee on Scientific and Technical Information, known as COSATI, of the Federal Council for Science and Technology, has had a Task Group on National Information Systems for the last four years. It has done much to provide the foundation for specific national information systems in a variety of scientific and technical fields. International groups are now moving rapidly in the direction of new computer-based information systems in a number of fields: biomedicine, physics, chemistry, highway research, critical data, water research, space, nuclear energy, agriculture, and others. There are literally hundreds of agreements between nations, bilateral or multilateral, to exchange scientific and technical information. The trend appears to be almost as explosive as the proliferation of literature.

Information technology is becoming faster, larger, and cheaper with the passage of months. The move towards data banks in industry, the government, the universities, and the professional societies is matter of record. The knowledge industries, it has been claimed, will very shortly be the largest industry in the United States. David Sarnoff once pointed out that information has become the building block of modern society. A lot of other astute observers have said the same.

In some inexorable way, we seem to be moving away from an era of information scarcity to a period of information abundance. This does not mean that all of the information will be worth storing. Far from it. But it will change our attitude towards the apparatus that gathers and stores it, and perhaps encourage us to engage in information birth control programs. I would hope that this shift in direction would be a matter of discussion in this important seminar. Electronic control of data is a far different problem than control of data that resides in locked filing cabinets. The skills of the people who need to safeguard electronically recorded data must be different and much more demanding.

Those of you who have been following the action and reading the minutes will know that there is a

fairly widespread concern in this country about the invasion of privacy by means of misused data banks in government and the private sector. The data collection trend has been gathering momentum, and I venture to say that each person in this room has personal data about himself and his family that would shock him stored away in somebody's computer. How secure these data are should be a concern of the individual and society. If your organization has not been more than passively worried about the possible mischief that can result from these files, it might be something you might want to study. I refer to banks containing data about people, more specifically: marriage, divorce, credit ratings, job history, personal references, traffic citations, misdemeanors, use of drugs, automobile accidents, and taxes, to name a few.

One of our COSATI panels is interested in this and similar problems; it is the Task Group on Legal Aspects of Information Systems. Some of you are familiar with yet another COSATI group, the Task Group on Dissemination of Information, which has completed its formal study and is now putting the finishing touches on its very comprehensive report. I am fully aware that the report will touch on a few tender nerves, pointing out that some of the dissemination practices of the Federal agencies ought to be upgraded. The Moss Act on freedom of information is another indicator of the temper of Congress, and therefore the people. Several months back, the famous anthropologist, Margaret Mead, and a group from the American Association for the Advancement of Science completed a report on secrecy. It carried a clarion call to all scientists to resist efforts to withhold scientific data. There was full recognition however that some information must be withheld, referring to security and proprietary information. But it was hoped that restrictions would be few and the time of withholding short and only materials that really ought to be so treated would fall into this category. Of course, scientists can be expected to complain, and do complain, about restrictions on their movement and disclosure of their findings to fellow scientists. Sometimes, the complainers are out of line, but every now and then the fault lies with people who do not intelligently follow their own regulations, or show a singular lack of flexibility.

Too often they follow the line—if in doubt, classify. Then somebody has to bail the department or agency out. One of the fruits of a myopic policy is the desire on the part of people in Congress to turn basic and some applied research over to "pure" outfits like NSF. Sometimes a few of us get the feeling that it would be a real boon if we could develop a litmus paper test for common sense in applying release rules. Let me temper this comment with the observation that I am talking about a very small minority. The trouble is though every time there is a confrontation it is magnified way beyond its size and importance; it becomes news, and news in this field usually is negative.

Some of the problem is compounded by the way the regulations and directives are written, quite apart

from the interpretation of their meaning. It is my hope that your study groups will take a hard look at the wording of directives and the export control laws applying to data to determine what could be done to make them more understandable and workable, if this is possible. If this is done, I urge you to consider the changing climate that I tried to describe earlier — information plenty rather than scarcity and the necessity of using new knowledge rather than safeguarding it.

Another part of the problem that needs ventilation and maybe a new approach is the uncomfortable relationship between scientists, engineers, managers and security people. If we asked the question, just how much of the scientific and technical material kept secure really deserves such treatment? I am inclined to the belief that we would get an embarrassed and mixed answer, depending on who gives the response. The security people are usually accurate when they say, "Look, we withhold only the material that the scientists and administrators classify as being in that category in the first place." Scientists and engineers, on the other hand, frequently claim that their views about what should be classified, how long, and to what extent are neutralized by security people. One of them recently told me, "It's a farce, the security people and the administrators make the decisions; I can buy some withholding of certain kinds of material and complete withholding of yet others, but the reward-penalty system we live under guarantees that a certain amount of information gets locked up just to play it safe. The trouble is, once we hide the material, it is damned hard to pry it out. Worse than that, with the turnover of scientists and others, the incentive to purge the files diminishes rather than increases with time."

When you discuss the matters with administrators, we get reactions like: "What can we do? It's up to the scientists/engineers and the security people. They have to make the decisions, not us. Besides, if you read the record you will find that nobody got his head lopped off in Congress by taking a conservative approach to release of information. Just about every country in the world wants to get the knowledge we create for nothing; why should we make it easy?

If I have not defined the position of each group accurately, I apologize. If I have over-stressed the negative aspects, it is to point out that it is devilishly hard to get good teamwork and cooperation, when passing the buck is so easy and convenient.

Just about a year ago, I gave a talk to a small government group involved in internal security. Some of you may have been there. Some of what I said then is still relevant today. After making it clear that our office did not advocate that information of strategic, proprietary and security content be freely disseminated, I went on to say a few things that might be worth repeating.

We favored the maximum exchange of knowledge nationally and internationally. We still do.

In a country with our kind of pluralistic society, withholding information for long periods is almost impossible; additionally it is a costly process. Moreover, few countries in

the world can use the advanced technical information that we generate in time to do us competitive harm. The half-life of competitively useful data is getting shorter and shorter with the passage of time, and it does us no real harm to empty our information banks earlier in time. Perhaps it is not flattering, but a considerable amount of information we generate is not that good. We might be better served if we made it more easily available to fill and sometimes clog the collection apparatus of potential enemies and erstwhile friends, just as its forms fatty matter in our own information arteries that we could do without.

Additionally, I pointed out that we are and will continue to be dependent on knowledge originated in other countries. Inventions such as sonar, color TV, jet engines, the Kaplan turbine, zoom lenses, polyester fibers, radar, continuous casting of metals, high-speed phototypesetting, holography, and variable geometry aircraft wings are examples. The knowledge came from overseas, but American technological know-how did much to develop them. We have only about six percent of the world's population, and it is dubious to expect that we can corner the world's knowledge in the long run. It is dubious if we can construct a real fence our knowledge bank. Our unique ability in the United States is in exploiting new developments more rapidly than other countries, without denigrating our capacity to uncover new and exploitable basic knowledge. I think that this statement is still accurate. I concluded that talk with the hope that at least in our government where the division of duties between those who generate and disseminate data and those who are charged with safeguarding them are somewhat separated some way will be found to work with better teamwork as we find our way through this transitional period.

Now I must bring my talk to an end. At this point, I would like to affirm the value of groups such as yours. Even under ideal conditions, which never seem to exist, the task of those who have the chore of classifying information is hard and unappreciated. During a period of change such as we are undergoing, it becomes tougher. You are prone to be criticized when things go wrong and take the rap even when this is not justified, but this is part of the game, though painful. Policies and practices in the security area will always be challenged, and I do not think that you should leave this game for others to play all by themselves.

In the last couple of days, we witnessed a triumph of American technology in getting two men to the moon, and we pray that they return safely. In a way, I believe that all of us should be proud of their accomplishments and hope that something that we have done, and I include classification management, made some kind of contribution to this unparalleled event.

Gentlemen, I wish you an outstanding seminar.

PANEL – DISSEMINATION AND TECHNOLOGICAL PROGRESS

Colonel Currie S. Downie
Office of Aerospace Research, USAF, Moderator

Downie: The technological progress of a nation is largely determined by its ability to generate and use scientific knowledge. In turn, both functions depend heavily on the wide availability of existing knowledge to the members of the technological community. Thus, effective dissemination of the scientific and technical information is rightly viewed as one of the most important responsibilities of the nation's R&D institutions.

The Federal Government, through its agencies, is the biggest of these institutions. About 16 billion dollars in support of U. S. R&D efforts come from this single source. Effective dissemination of Government-sponsored scientific and technical information and its effective use in technological innovations is therefore high on the list of national priorities.

At the same time, the government has the principal responsibility for providing for common defense against potential enemies. Given the present unsettled world environment, and the fact that superior military power is so dependent upon science and technology, it is necessary that the government exercise caution and sound judgment in determining how much of its technical information can be prudently divulged.

This situation is not new for our government. Until recently the criteria for dissemination and withholding of information have been largely determined by individual officials of the Executive Branch, and their decision was usually final. In recent years, however, something new has been added. Congress passed Public Law 90-23, the so-called "Freedom of Information Act," which added a new dimension to the decision process and established explicit criteria for the guidance of both government officials and the public.

In general, the law is another milestone in the trend toward wider dissemination of government-generated or government-held information. It recognizes the importance of and necessity for withholding certain information and spells out the conditions under which it can be withheld. But it also establishes the important principle that disclosure be the general rule rather than the exception. It stipulates that all individuals have equal right of access to government information. Moreover, it imposes on the government the burden of justifying the withholding, and frees the individual from justifying his request.

The law was established to deal with all types of information, primarily that concerned with administrative matters, but it also deals with technical information. At the same time the need to review government dissemination policies, procedures, and mechanisms has been recognized for sime time by the Committee on Scientific and Technical Information (COSATI) of the Federal Council on Science and Technology. Thus, the

combination of these two factors led to the establishment of a special COSATI Task Group on Dissemination of Information. The job of this group was to review the policies and practices of the federal agencies, examine them in the light of the new law and the needs of the U. S. technical community and recommend the *practical* steps needed to fulfill the government's responsibility.

Dissemination, as defined in Webster's New International Dictionary, is the act of disseminating or state of being disseminated; diffusion, as of ideas, beliefs, for propagation and permanence. As used by the task group in the context of this report it means the release, transfer, spread, diffusion or exchange of information in all its forms: oral, written, tapes, photos, films, drawings, documents, reports, publications, etc. Antonyms to dissemination are: withholding, restricting, or limiting full disclosure and distribution of information.

After two years of study, interviews, and analysis the task group concluded that despite the significant progress of the last decade, much remains to be done. The principal areas where concerted efforts are required are in the definition of performance criteria, the strengthening of certain legislative mandates, the full implementation of the clearinghouse concept and the improvement of the mechanisms for implementing Public Law 90-23 and the policies of the Federal Council for Science and Technology.

The task group wishes to call attention to a number of concepts developed in earlier studies which have guided the collective thinking of the Task Group. These concepts can be viewed as the principal national requirements for dissemination which must be met if significant and meaningful improvements in Government dissemination practices are to be achieved.

1. All government reports should be freely available to the U. S. scientific and technical community unless specifically exempted by the "Freedom of Information Act" (5 USC 552). The only exceptions are stipulated in the Act itself and include the following categories which apply to scientific and technical information, matters that are:

Specifically required by Executive Order to be kept secret in the interest of the national defense or foreign policy (Exemption 1).

Specifically exempted from disclosure by statute (Exemption 3).

Trade secrets and commercial or financial information obtained from any person, and privileged or confidential (Exemption 4).

2. The transfer of information is an inseparable part of research and development, and the control and dissemination of information resulting from such research and development is a vital element of the agencies' responsibility. This position has been advocated by the President's Science Advisory Committee (Weinberg Panel) and confirmed by the Federal Council policy which declares that "publication of research results is an essential part of the research process and should be treated as an authorized expense against Government grants and contracts.

3. The Federal Government is re-

sponsible for insuring that there exists in the United States at least one accessible copy of each significant publication of the worldwide scientific and technical literature. This also includes the responsibility for appropriate acquiring, announcing, processing, and making accessible the significant worldwide scientific and technical literature to qualified individuals and organizations in the United States. These recommendations were first enunciated in the 1965 System Development Corporation report and partially included in "Policies Governing the Foreign Dissemination of Scientific and Technical Information by Agencies of the U. S. Federal Government," dated 31 Jan 1968.

4. The technical information of government-produced or government-sponsored technical documents must be made available within a reasonable time and without unusual procurement effort by the potential user. The task group assumes that the criteria of reasonable time and unusual effort are met if:

a. A delay of not more than two weeks occurs between the request for information or documents and its receipt.

b. The cost of the requested documents is not greater than the cost of ordering and purchasing commercially available books or documents of equal length and complexity.

c. A delay of not more than six months ensues between the acceptance of a technical document manuscript and its availability through the government document clearinghouses and centers, or through the open professional journals.

d. A delay of not more than one year occurs between the conclusion of research and the publication of final research results. (Interim research findings should be made available within six months as in c. above.) Where patent considerations are involved a somewhat longer period may be justified.

In view of these criteria, the task group considered the specific policy and operational requirements which would have to be fulfilled to carry out the accepted government responsibilities. Thus, there is a requirement for:

1. Each federal agency to formally acknowledge that the dissemination of its research results to the scientific community is its responsibility.

2. Criteria and guidelines to assure uniform and consistent interpretation and execution of these basic responsibilities by the agencies.

3. Conspicuous and well publicized points of access to Government-produced technical literature.

4. Simple and easy procedures for identifying, requesting and obtaining government-produced technical reports.

5. Greater resources to improve the announcement and availability of technical literature and/or better allocation and use of the resources already available.

6. An effective executive mechanism to decide on the desired level of improvements and for directing the implementation of accepted programs.

7. Periodic evaluation of the existing dissemination practices and programs to insure that they continue to meet the demands of the scientific and technical community.

8. Frequent review of classified and otherwise limited technical literature to insure prompt release when the need for protection no longer exists.

9. A comprehensive federal policy concerning the dissemination of Government technical information.

In reflecting upon these requirements, the task group found evidence of considerable progress and many improvements since Senator Humphrey first highlighted some of the problems involved with dissemination of Government information. Certain improvements resulted from the expression of Congressional interest and concern; others were stimulated by COSATI, or at the initiative of single agencies; and still others from the cooperative efforts of several agencies. More precisely, the progress is evident in this partial list of achievements:

- Support of society journal publications through adoption of the Federal Council for Science and Technology policy which authorizes payment of page charges for journal articles.
- Federal Council policy which commits the government to insuring orderly acquisition, availability and accessibility of world-wide scientific and technical literature.
- Development of guidelines to format standards for scientific and technical reports to improve or achieve wider usability of reports.
- Adoption of microfiche standards.
- Development of subject category lists to aid classification of government-wide scientific and technical information.
- Cooperative efforts of AEC, DOD, and NASA in minimizing duplication by the interchange of documentary and bibliographic information and by providing input to the Clearinghouse for Federal Scientific and Technical Information.
- The programs for transferring government developed or sponsored technology to the industrial and private sector, especially by NASA through its Technology Utilization Program and by the Office of State Technical Services of the Department of Commerce.
- The establishment of a system of focal points for scientific and technical information within the federal agencies.
- The selective dissemination of microfiche by the Clearinghouse, the Defense Documentation Center, AEC, and NASA.
- Establishment and support of federal information analysis centers.
- Strengthening and expanding the role of the Science Information Exchange.
- Development of the Interagency Data Exchange Program (IDEP).
- Creation of Educational Research Information Centers (ERIC).

The list does not include a number of less tangible, nevertheless very important changes in the national attitudes toward the scientific and technical information problems, from the previous indifference to the present extensive involvement as evidenced by the committees and working groups, both inside and outside of the government. The work of COSATI, Scientific and Technical Communications Committee (SATCOM), and the recently organized Information Industry

Association provide concrete evidence of this concern. The above listing also omits many on-going efforts to establish national and international systems for information networks to further the availability of scientific and technical information.

Nevertheless, many problems remain, and at times appear to be beyond the possibility of any reasonable solution. The task group will explore the remaining impediments to the dissemination of scientific and technical information and the associated problems, and consider a range of possible solutions.

ALEXANDER G. HOSHOVSKY
Office of Aerospace Research, USAF

As the initial step, the task group examined seventeen previous government studies concerned with the flow of technical information in the United States. All of these studies found fault with government dissemination procedures and practices. Each study presented an array of solutions. To date some recommendations have been implemented; others are pending adoption. Still other recommendations have been ignored or rejected.

In reviewing these studies the task group found a number of comments and recommendations on the dissemination of information which are worth repeating.

In 1962, Senator Hubert H. Humphrey forcefully called the Federal Government's attention to his finding that:

> The lack of an integrated system for the dissemination and exchange of scientific and engineering information . . . results in duplications, useless expenditure of funds, and other shortcomings that impair the efficiency of various federal research, development, test and evaluation programs involving billions of dollars.

The Crawford Report of 1962 presented a strong indictment of the mishandling of the government's report literature:

> The absence of systematic coordination among R&D agencies precludes optimal initial reproduction, distribution and use. Some agencies . . . attempt regularly in the production process to anticipate all current needs for documents so that optimal press runs can be made during initial reproduction for users, stockpiles and other purposes. In most agencies . . . no such coordination of agency-wide or government-wide needs is attempted regularly. By improved coordination at this stage in the production process . . . appreciable speed up of initial distribution of information and significant reduction in workloads could be effected in secondary distribution and distribution of single document copies. Initial reproduction and distribution need to be kept under effective, continuing control to make sure at the same time that excessive quantities are not automatically produced and that scientists and engineers are not automatically burdened with irrelevant materials.

The Crawford Task Force also observed that the policies of those agencies which rely wholly on conventional publications for the dissemination of

information generated in their R&D activities are not satisfactory because any chance factors influence the results and effectiveness of these policies. The absence of supplemental methods to ensure accessibility and availability of information generated under government sponsorship and not published in conventional journals was seen as a serious weakness in the management of technical information by those agencies. Therefore the task force group recommended establishment of a federal clearinghouse for information covering planned and active on-going R&D efforts of the Government, as well as the documented R&D results. The agencies were expected to maintain comprehensive up-to-date indexes of their own current on-going R&D efforts and provide prompt and appropriate information about those efforts to the clearinghouse for processing and authorized dissemination.

In 1963, the widely cited Weinberg Report pointed out that:

> Barriers do exist in the flow of reports and other documents . . . these must be discovered and removed. Perhaps most important, many contractors and lower level administrators consider reports as only incidental to the development of a piece of hardware. If the hardware works well, why bother about the report? The contractor is selling equipment, not information, and the project officer is judged by the results, not by the report.

The Weinberg Panel regarded the excessively rigid interpretation of security regulations as an undesirable barrier to dissemination of information. In the face of a clear recognition of the asymmetry between the way the communist and noncommunist nations handle technical information, the panel felt that the interests of the United States might be better served by the application of a more liberal policy which in balance should lead to more security, not less. Not being sure of the impact imposed by the DOD and AEC regulations, the panel recommended that an *ad hoc* group of the Federal Council's Committee on Scientific Information (now COSATI) further examine this question.

With respect to a contractor's proprietary rights in government procured information, the panel expressed the belief that such rights posed tangled, difficult legal questions beyond the matter of information transfer. The panel was of the opinion that the efforts of developing more uniform government-wide policies on patent rights in government research and development contracting should be expanded to cover proprietary nonpatentable rights. Such policies would aid contract administrators in deciding whether contractors were justified in withholding information.

Following the first comprehensive accumulation of data relating to federal dissemination practices, the Elliott Committee in 1964 concluded that:

> There may be more information being generated than can be effectively handled; there may be more arteries than are needed to carry it. The greater the quantity of new research information, and the more widely it is dispersed, the harder it is for anyone to find what he is seeking.

The following year (1965) a special panel of the Federal Council for Sciences and Technology under the chairmanship of J. C. R. Licklider concluded that from the point of view of a scientist or engineer in a university, industry, or in government the arrangements for handling scientific and technical information did not stand out boldly and in clear relief, and did not present themselves as a convenient or effective tool or as a well integrated and readily comprehended system. Further, the panel felt they were neither well understood nor effectively used by most scientists and engineers. The arrangements were too complex, too dispersed. In the panel's view the government's documentation system should present a "conspicuous front door and simple rules for ringing the bell."

In 1965 and again in 1966 the Department of Defense carried out the so-called "DoD User Needs Studies," which found that, among industrial users, more than one of three document requesters run afoul of proprietary or security restrictions, with 60 per cent involving security. Quantitatively, the studies reported that timely awareness and timely acquisition posed problems for more than two out of five users. Approximately 20 per cent of the difficulties stemmed from lack of timely awareness of needed information, and over 50 per cent involved delays in acquisition of information. Timely awareness difficulties were evenly divided between internal and external company sources of information, while timely acquisition difficulties were much more often external than internal.

In 1965 the System Development Corporation (SDC) issued the first comprehensive report sponsored by COSATI, entitled "Recommendations for National Document Handling Systems in Science and Technology" which concentrated primarily on document storage and retrieval. The first two recommendations emphasized availability of information:

1. The Federal Government has the responsibility to assure that there exists within the United States at least one accessible copy of each significant publication of world-wide scientific and technical literature.
2. The Federal Government has the responsibility to see that there is appropriate acquiring, announcing, processing, and making accessible the significant world-wide scientific and technical literature to qualified individuals and organizations in the United States.

Insofar as this task group could ascertain, only the first recommendation found an expression in a federal policy by the Federal Council for Science and Technology. The second recommendation which is more closely related to the government's responsibility for dissemination, has yet to be accepted.

In a 1966 follow-on "Study of Abstracting and Indexing Services," the Systems Development Corporation reported to COSATI that it found (1) a general lack of knowledge on the part of users about proper use of available services; (2) problems of quality and timeliness of abstracting-indexing services—in the face of rising costs, personnel shortages, and a lack of information on the part of the services regarding user needs; and (3) in-

adequate information within Government in the areas of costs, data upon which to base standards, and information overlaps.

In response to a 1966 Congressional proposal to confer exclusive rights on a copyright owner with respect to reproduction of his work for input into an information system, COSATI appointed an *ad hoc* group to prepare a special analysis of copyright problems as they impacted upon information systems. This group reported that:

> The proposed copyright bill . . . may hinder the development or maximum efficient use of national information systems primarily because of the burden it imposes of contacting the owner of the copyright on each item of copyrighted material used by the system which is not covered by fair use or otherwise exempted, and securing his permission to use the material.

Further, the *ad hoc* group recommended:

> . . . input into information systems not used for profit be exempt during an interim period from the requirements of the copyright law. Since such systems are now and surely will be for the next several years in a very primitive stage of development, exempting them from copyright liability should not deprive copyright owners of significant amounts of revenue. At the same time, an exemption will guarantee that research in this area is not hindered in any way by a requirement that users of the system must secure permission from a copyright owner before they may use copyrighted material.

Finally, this *ad hoc* group offered as solutions (but not as recommendations) statutory licensing and a voluntary clearinghouse to arrange for copyright permissions.

In August 1967 a COSATI-commissioned study on "Oral/Informal Communications" explored and defined the boundaries of informal communication behavior, i.e., personal conversations, office conferences, telephone calls, meetings, and the like. The study, which was conducted by the American Institutes for Research (AIR), confirmed the earlier findings that informal communications play a large and important role in research planning, evaluation of data, sharing of knowledge about R&D methods and techniques, evaluation of experimental data and the acquisition of state-of-the-art information. It also addressed itself to certain obstacles which inhibit a full exploitation of this mode of communication.

Accordingly, the study found that many scientists were not permitted adequate use of the telephone because of administrative restrictions which often exist in many organizations, despite the fact that the telephone is still the best substitute for travel. The study also found that the fundamental reasons for making visits to other laboratories are not adequately comprehended by management, and permission to travel often is withheld to the detriment of research progress. Such visits for the purpose of studying equipment fulfill a fundamental need for information which presently cannot be adequately met through other means.

Several of the recommendations advanced by AIR were especially rele-

vant to improvements in the dissemination process. More liberal policies were suggested on long distance telephone calls supported with additional funds for the use of telephones. A systems study was recommended with a view toward establishing a nationwide R&D communication network capable of carrying voice as well as graphic messages. Also recommended was the establishment of an easily accessible index of research advisors to aid in the selection and contacting of the most appropriate and knowledgeable people. The final recommendation called for greater publicity for the government's research information services to try to overcome the unawareness of many researchers of the available information dissemination services.

The COSATI-initiated study of the "Role of the Technical Report in Scientific and Technological Communication" was carried out in 1967 by the Passman Task Group. While examining the role and use of technical reports generated by government, industry, and universities, it also provided some insight into the nature of dissemination problems.

The Task Group observed that the government, as a sponsor of tremendous amounts of scientific and industrial research, is primarily interested in the exploitation of this information for solving specific problems and assuring that contract goals are met. As a philosophical principle, the government now recognizes the potentially wider significance of any given effort to other groups and to other problems. Thus, assuring availability of technical reports issued under contract obligations through clearing houses is an important step in the dissemination of information which might not be expected to occur voluntarily through the "open literature" in all cases without such intercession. A deterrent pointed up by the panel, however, was:

> . . . the compartmentalization of research support through numerous project offices and agencies results in widely different dissemination policy interpretations. Where agencies have statutory responsibility for information dissemination, or an agency administration is aggressively pushing in this direction, the situation is far superior to those cases where such policy is generally ignored or only given lip service.

The report recommended that the government insist upon full and high quality reporting of work done under government contract and that:

> Adequate time and resources under the contract must be allocated to the review function. Concern for the significance of the results of an effort, and their dissemination to a greater audience than those close to the immediate project, demands that this review include a concern for the writing, editing, data findings, dependent references and objective statements of the context and limitations of the results.

It was suggested by the group that the functions of:

> Dissemination evaluation and review of technical reports should be explicitly added to the responsibilities of government project officers as an assignment from agency directors and administrators. These functions would be considered along with the project effort in the evalu-

ation of the project officer's administrative performance.

In examining the question of whether present federal technology transfer produces a net benefit to the economy in comparison to costs of operation, the Senate Subcommittee on Science and Technology of the Select Committee on Small Business (Randolph Committee) concluded in 1968, that a significant proportion of government-generated technology is not accessible to all potential users. The varied information handling techniques were found to be incompatible and uncoordinated, and counseling, referral, and dissemination services were found not to be equally available to all regions of the country, to all industries, or all businesses. The committee also felt that the Mutual Security Act, Title 22, USC, Section 1934, and the Export Control Act, Title 50, USC Appendix, Section 2021, as presently constituted, have the effect of restricting public announcement of a significant number of technical reports, thus denying to American business access to useful publicly developed technology. The review of these acts was recommended.

In addition to specific recommendations relating to information analysis centers and creation of a nationwide system of referral contact offices, the subcommittee recommended evaluation and compaction of raw information into interpreted, readily-usable packages conforming to uniform, high-quality standards.

In 1968 the COSATI-sponsored study of "Scientific and Technical Data Activities in the United States" found that the time lag between data generation and dissemination, utilizing traditional publication channels, may be from two to five years. Moreover, the study noted (just as the earlier Systems Development Corporation study had observed) that while science has fostered wide dissemination and accessibility to scientific data, both private industry and the Federal Government's mission-oriented agencies frequently restrict the distribution or accessibility of the data they generate. This is due, in some instances, to security or proprietary considerations; in others to insufficient incentives to expend Government funds or efforts to make the data available to other users.

Among the many recommendations submitted by this study, three impinge directly on improvements of the communications process. The first recommendation proposes establishment of a National Index of Scientific and Technical Data, consisting of subindexes covering data resources of interest to different user communities. The second recommendation advocates adoption of a federal policy statement to encourage the availability and accessibility of scientific and technical data to as many potential users as possible. The policy should not conflict with full recognition of the property rights of individuals or organizations. Rather, it should be promulgated with a specific delineation of private data (data which an organization or individual does not desire to disclose or release), proprietary data (data which the owner or possessor will release under prescribed conditions such as payment of a fee), and public data (data for which ownership and possession is in the public domain). Government support should

be given to efforts for removal of the barriers which result in data being restricted, when in fact, the owner or holder has no objections to use of the data by others.

The third recommendation proposes federal action to guarantee that data generated under government sponsorship are managed to assure maximum use. This would be accomplished by requiring direct, even if minimal, effort to carry out the objective on all federal research and development programs, and would be supplemented through a central clearinghouse which would support the special operations required to move data from restricted or limited use contexts to those in which data has broader visibility and greater use potential.

In 1968, the Department of Commerce appointed an Ad Hoc Committee to study and make recommendations on Recommendation XXIX and XXX of the "Report of the President's Commission on the Patent System." The Urbach Committee on Patent Documentation, in considering dissemination aspects of patent information, concluded that:

> Access to the patent literature today is difficult for any but the skilled patent practitioner. The single location of the public search room in the Washington, D. C. area, the cumbersome patent classification system which is unintelligible to the uninitiated and the lack of clarity in the patent specifications themselves all contribute to inhibiting the broad use of the patent literature by the technical public.
>
> The Patent Office itself devotes almost no effort to considerations of the problems of dissemination of patent information to the general technical public. It is difficult to determine which Patent Office official is responsible for this function. The Patent Office's Office of Information Services has made some efforts to disseminate information about the patent file and the search tools available for its use. Although some limited success has been achieved by this small program, the dissemination of patent information is clearly regarded as an unimportant by-product of internal Patent Office operations.

Also in 1968 the Department of the Air Force sponsored a study on the "Diffusion of Abstracting and Indexing Services for Government Sponsored Research," which reported that federal documentation centers may be doing a creditable job in supporting the missions of their agencies, but:

> it is obvious that thousands of research-oriented industrial organizations, educational and nonprofit institutions and private individuals, do not receive the federally-produced abstracting and indexing services and, what may be more significant, have no knowledge of their existence.

Among the most recent publications which have dealt with dissemination problems is the recently released report of the Committee on Scientific and Technical Communication (SATCOM) of the National Academy of Sciences. The problem of dissemination is treated in a number of sections, but of greatest relevance here is its finding that obstacles to effective utilization of secondary (indexing and abstracting) services result primarily

from a lack of awareness of the existence of such services, difficulties in gaining access to them, and in complexities of their use. Concurrent with the difficulties of obtaining these services themselves are the problems of gaining access to documents that they identify, particularly technical reports and other federal documents. SATCOM finds that persons wishing to purchase, borrow, or obtain copies of documents from federal agencies discover that there are a multitude of agencies responsible for their sale, loan or duplication, and a wide variety of procedures to be followed.

JAMES J. BAGLEY
U.S. Naval Research Laboratory

The key findings of major studies on the obstacles to dissemination of scientific and technical information and the progress that has been made to date have been discussed previously. What follows is concerned mainly with those areas of dissemination impediments wherein additional progress may be made.

Major obstacles to effective dissemination of information arise from the lack of clear policy guidance for the intentional withholding of information by means of security classification, limitation statements, etc., and also from the technical and operational problems involved. These include obtaining adequately trained and educated personnel and sufficient funding to perform the necessary abstracting, indexing, and other required tasks, and improved mechanisms for dissemination of information.

As previously mentioned, the task group finds the most significant exemptions from disclosure, as provided by Public Law 90-23, the "Freedom of Information Act", exist in matters that are:

- Specifically required by Executive Order to be kept secret in the interest of national defense or foreign policy (Exemption #1).
- Specifically exempted from disclosure by statute (Exemption #3).
- Trade secrets and commercial or financial information obtained from a person, and privileged or confidential (Exemption #4).

Additional impediments to dissemination are encountered in the following areas:

Where the means of publication, printing and servicing requests for documents are inadequate.

Where access to unclassified technical information requires specific authorization.

Where informal/oral communications are inhibited by administrative restrictions, and/or funding limitations.

There is a deep and continuing conflict in U. S. policy between the need for greater public dissemination and the equally pressing need for official secrecy. Any attempt toward resolution of these diametrically opposed policies undoubtedly would involve achieving a consensus. In the final analysis, each case for disclosure must be resolved on its own merits—whether the arguments for withholding are stronger or better justified than the arguments for release.

Significant progress has been made in the last six years in the control of classified information by the defense agencies. The Department of Defense in 1963 instituted a Classification

Management program which established criteria for applying security classification to information, limited the number of individuals authorized to classify information, and required the generation of classification guides for the edification of individuals doing classified work. The purpose of these guides is to establish, with as much precision as possible, what information on a particular project is classified, the level of classification, and the reason for the classification. It also established the period of time the information is classified. For example, the information may be exempt from automatic declassification, it may be downgraded but not automatically declassified, or it may be automatically declassified after a period of time, generally twelve years or earlier, depending on the circumstances. The automatic downgrading and declassification feature of the program is effective, and has been placed into effect by all the defense agencies. Ultimately, this facet of the classification management program will go far in reducing the great volume of classified information withheld by the defense agencies. However, more progress is needed. *There is still no system of incentives to downgrade or declassify information; there is no penalty for overclassifying information. There are no mandatory requirements for review of classification decisions and as a consequence unnecessarily large quantities of classified information are being created.*

Classification, when applied to information, is time-limited. Its purpose is to gain lead-time, to protect information critical to military operations, and to protect technological advantage. Thus, classified information should be regularly reviewed and downgraded, as time depreciates the value of the information to national security.

Dr. Vannevar Bush summarized his views of the relation of security to research in his book, *Science, the Endless Frontier,* in 1945, as follows:

> "Our ability to overcome future enemies depends upon scientific advances which will proceed more rapidly with diffusion of knowledge than under a policy of continued restriction of knowledge now in our possession."

Dissemination of scientific and technical information within that portion of the government concerned with national defense is and will continue to be a problem; a problem which, in the simplest terms, is reduced to one question—Will dissemination help or hurt the national defense? Although there is a general consensus within the technical community that the real security of the United States would best be served by stringent limitations on the use of secrecy, this question deserves far greater study than is possible by this task group.

There will always be a need to protect information about people and institutions. The government must have access to private information and the donors of the information must be assured that their private information will be protected from improper disclosure to competitors.

It is certain that some controls on the dissemination of scientific and technical information will continue. In this respect the Committee on Science in the Promotion of Human Welfare of the American Association

for the Advancement of Science made an in-depth study of "Secrecy and Dissemination in Science and Technology" and concluded: "In our view it is not secrecy as such that threatens the integrity of the scientific process, but excessive and inappropriate uses of secrecy. . . ."

Among the major statutory obstacles to dissemination are certain provisions of the "Export Control Act of 1949" and the "Mutual Defense Act of 1951". These acts prohibit the export of articles, materials or supplies, including *unclassified* technical data or any other information pertaining thereto, to any nation threatening the national security of the United States. It is required that countries receiving military, economic or financial assistance from the United States agree to embargo shipment of certain materials to nations threatening U. S. security under penalty of withdrawal of such assistance. The acts are administered by the Department of Commerce which maintains a Comprehensive Export Schedule and issues Export Bulletins of controlled articles.

Obstacles are found in the provisions of the Mutual Security Act of 1954 which limits the export of arms, ammunition, implements of war and unclassified technical data or information relating thereto, and is administered by the Department of State via its International Traffic in Arms Regulation (ITAR). In the International Traffic in Arms Regulation, Title 22, CFR 125, technical data is defined as:

"a. Information concerning an article on the U.S. Munitions List which enables its use, operation, maintenance, repair, overhaul, production or manufacture, or

"b. Research, development, and engineering technology concerning an article on the U.S. Munitions List, or

"c. Any technology which advances the state-of-the-art or established a new art in an area of significant military applicability, or

"d. Information as defined in Title 22, CFR 125.03 Classified Information."

In the Export Control Act, the definition is limited primarily to information related to production or manufacturing—technology rather than research-related. In the latter case (the ITAR), the definition is so broad that any information generated or created by a defense agency could be included. A definition of the term "significant military applicability" is conspicuous by its absence. The Department of Justice added to the statutory confusion by its opinion with respect to Section 552(b)(4) of the Administrative Procedures Act in which it said that: "An important consideration should be noted as for formulae, designs, research data, etc., which, although set forth on pieces of paper, are significant not as records but as items of valuable property." These may have been developed by or for the government at great expense. There is no indication anywhere in the consideration that the Congress intended, by Subsection (c), to give such property to every citizen or alien who is willing to pay the price of making a copy. Where similar property in private hands would be held in confidence, such property in the hands of the United States should be covered under exemption 4: "The provisions

of this section shall not be applicable to matters that are . . . trade secrets and commercial or financial information obtained from any person and privileged or confidential."

These guidelines have been variously interpreted by the defense agencies when release concerns advanced technology which, in the hands of some foreign countries, could significantly advance their military readiness. In a few instances, military departments have taken the position that all R&D information generated has potential intelligence value and could enhance the military posture of a potential enemy.

In 1965, the Department of Defense issued a directive to apply distribution limitation statements, of varying degrees of control, to technical reports. Although the directive was applicable to both classified and unclassified information, its most detrimental effect is on the dissemination of unclassified information. The net effect of the directive is that the flow of unclassified information to the technical community outside the government has been greatly reduced. One of the principal offenders is Distribution Statement #2 which reads: "This document is subject to special export controls and each transmittal to foreign governments or foreign nationals may be made only with prior approval of (controlling DOD office)." The basis for applying the statement is: "Information included that was furnished by a foreign government; commercial competition with foreign firms; protection of technical know-how relating to critical products or manufacturing processes, tests and evaluation of military operational weapons systems and installations and other technology restricted by U. S. Mutual Security Acts." Major commands of the military departments have issued directives requiring that all technical information generated be, as a minimum, marked with this statement, because all information is generated as the result of military requirements and is considered to have "potential intelligence value." Some of these commands have also issued directives removing from subordinates the authority to release technical information to the public. It certainly cannot be denied that some unclassified information has intelligence value, or that some information should have been classified, or that there is a "potential" risk in the publication of some information, or that there have been instances of improper dissemination. However, the means employed to achieve control often seem inappropriate.

While it is a generally accepted fact that the purpose of military research and development is to improve U. S. military posture, it is equally true that the benefits to the national economy of military R&D cannot be predicted with any degree of validity. However, history indicates that several items developed for military purposes have had wide economic benefit — atomic energy, radar, and microelectronics, for example. Restrictions on the dissemination of such information is contrary to Congressional interest in technological transfer or technology utilization, the passing of knowledge to industry to improve technology, and for development of new skills to enhance the national economy.

The inevitable result is increasing

pressure by technical societies, the technical community, universities, and members of Congress to correct the situation. The point may be illustrated by the fact that in FY 1967, 45% of the unclassified information received by the Defense Documentation Center was restricted from public dissemination by enforcement of the International Traffic in Arms Regulation by the Department of State, and the Export Control Acts by the Department of Commerce.

The core problem is that the effect of the Export Control Acts and the International Traffic in Arms Regulation on the Department of Defense is, at the decision-making level, misunderstood. Because of this, honest individuals, knowing that they will not be criticized for withholding information, but that they may be criticized for inappropriately releasing a technical document, tend to take the easy way out and limit dissemination. *What is urgently needed, and what is recommended elsewhere in this report, is that COSATI convene an interagency committee to review the Mutual Security Act and the Export Control Acts. These laws as they are now implemented have the net effect of denying technical information to American business and the general public.*

A special area of concern is the DOD practice of limiting access to technical documents by its distribution statements. Especially troublesome are distribution statements #4 and #5 which may have little relationship to the exemptions authorized by the Freedom of Information Act. Statement 4 limits distribution to DOD only. Statement 5 requires the specific permission of the originator before distribution may be made by the Defense Documentation Center. The process by which a requester may obtain a report controlled by Statement 5 is both cumbersome and time-consuming. According to Mrs. S. O. Jones of the McDonnell-Douglas Corporation, at a presentation to the National Security Industrial Association in Los Angeles on 7 May 1969, documents marked with Statement 5 take an average of two and one-half months to obtain. Also, some originating organizations do not even take the trouble to reply to the letters requesting authorization to obtain the documents, since few DOD personnel are familiar with DDC Form 55 and know what to do with it. Here, the task group believes that *DOD should establish an appellate process by which requesters may (1) obtain answers promptly to inquiries and (2) appeal disapproval notices received from originating agencies without explanation.*

The Copyright Law poses a dilemma for the dissemination of government sponsored research. Ideally, information should flow freely from scientist to information publisher to information processor to user. The Copyright Law functions to assure both the author and the publisher a material return for their efforts as well as to protect the integrity of the author's work. However, a large part of the R&D is sponsored by the government, which has a policy that information developed at taxpayer's expense should be freely available to anyone. When government-sponsored research is published in copyrighted journals, the taxpayer is bound by the

provisions of the law. When information is published by the sponsoring agency, it is freely available. With the total numbers of professional and other journals now in excess of 35,000 and the costs of journals rising each year, not many libraries can afford to have an extensive journal collection which covers all government-sponsored research.

Another problem is how to deal with translations of copyrighted material, particularly since it is estimated that forty-five per cent of the world's scientific literature is in a language other than English. The problems arise not only from the availability of translators, but in making a translation widely available, because of the probable violation of the Universal Copyright Law and the difficulties in getting a copyright release from the originator.

Congress authorized revision to the 1909 Copyright Law in 1955 and since that time there have been many hearings and studies on this complex problem with little substantive progress. This task group sees little point in reiterating the arguments brought out in these studies beyond urging that COSATI attempt to establish a position on the subject and be prepared to furnish advice to Congress. The COSATI Task Group on Legal Aspects is currently studying this problem.

The Federal Government must have information about what the contractor proposes to do and how charges are to be paid, while business organizations have a right to keep their internal affairs concealed from the view of competitors. Proprietary information about contractors and potential contractors to the Federal Government — cost estimates, proposed techniques, etc. — which are matters a business organization does not want to become known to competitors, must be protected.

The complexity of public business is such that even minor policy issues can be expected to engage the attention of several departments in the Executive Branch, and many bureaus and other sub-units within those departments. The setting forth of the various alternatives supported by technical information and the reaching of logical authoritative decisions involves many organizations and many people. The decision-making process generates a number of draft papers and internal memoranda which are written neither with a balanced viewpoint nor with a clear exposition for the uninformed outsider. To make all of these papers available and understandable would impose severe burdens upon routine governmental business. More importantly, those developing the policy papers should be free to discuss the issues without feeling the need for building in the defenses and reservations that would be called for in public releases dealing with necessarily controversial issues.

The Government Printing Office (GPO), an element of the Legislative Branch of the Government, "has a two-fold responsibility with respect to collecting and disseminating scientific information: (1) reporting on its internally sponsored research and development projects, and (2) selling Government publications . . . The Public Documents Division is responsible for distributing and sale of Government publications printed by GPO

and for compiling and issuing official catalogs and indexes announcing the availability of all Government reports not confidential in nature, produced both in and out of GPO. This Division has no jurisdiction over the decision to issue any of the publications, nor can it impose limitations on the distribution. An inaccurate statement of the function of the Public Documents Division appears in the U. S. Governmental Organization Manual, as follows: "The Superintendent of Documents is the sales agent for United States Government Publications." To be accurate, the following words should be added: "Printed by GPO." (The Clearinghouse sells those U. S. Government publications made available to it whether printed by GPO or elsewhere).

The official announcement media of the GPO, the *Monthly Catalog,* which lists publications printed by the GPO for federal departments, bureaus, agencies and the Congress does not include comprehensive listings from GPO field or regional printing plants. *This is a serious lack of bibliographic control.*

The task group has been exposed to the evidence of delays in getting publications printed by GPO. One agency, Health, Education and Welfare, reported it had formerly published a publication through the Chicago field plant of GPO, but when the distribution list exceeded the number permitted for a field office, HEW had to suspend publication since the central GPO office was so slow that the information was outdated by the time it appeared in print. Another example of the slowness in printing is a review of the *Book of Mars,* which appeared in *Science.* "The *Book of Mars* is such an excellent book that it's a pity it's virtually unavailable for purchase . . ., we ordered the book from the Government Printing Office more than three months ago. As of this writing, copies . . . still have not arrived."

There are still considerable delays in obtaining requested data from other agencies. For example, the task group received a letter from one individual who asks: "If in fact the government is really interested in its effectiveness of information dissemination then why does it take four weeks for the Patent Office to fill orders for patents?"

Copies of technical publications prepared by Congressional committees, those dealing with science and technology policy, etc., are sometimes extremely difficult to obtain, especially if the requester is not in the Washington, D. C., area. "Committee Print" reports, those printed in limited quantity only for members of the individual Congressional Committee, are a case in point. For example, this task group found it nearly impossible to obtain a copy of the report "Federal Statutes on the Availability of Information." Only a few copies of this report had originally been printed and there was one copy at the Library of Congress and one copy at the Archives building, neither of which could be loaned. Congressional reports dealing with science and technology should be deposited with the Clearinghouse where copies can be quickly made available on request.

While the major portion of the impediments discussed in this report relate to the formal document literature, the task group cannot avoid

those impediments which inhibit the smooth functioning of the greater (and perhaps more effective) dissemination process — oral/informal communication. Here the task group fully agrees with the postulation that new ideas (whether technical or nontechnical) are transferred by persons and not reports. And for people to do this effectively, they must operate in an environment which is conductive to inter-personal relationships — telephone, attendance at meetings, and personal visits to laboratories to acquire the knowledge they seek.

The communication of technical information tends to be a unique problem in that the required constant feedback and clarification in the process of communication is best done during a person-to-person confrontations. According to various estimates, more than 50% of the actual scientific and technical dissemination is done in this manner. The foundation of an environment conducive to effective communication is the freedom to use the telephone and to travel. Here the task group has found restrictions usually imposed by nontechnical administrators throughout the government who fail to appreciate the effects of these restrictions on technological progress in their own agencies as well as the nation as a whole. It is unfortunate, for example, that travel which is usually an identifiable line-item in an agency's budget is often the first to be cut during periods of severe funding limitations, often without adequate thought about its effect upon the technical communication process.

The task group finds that despite the considerable advances and improvements that have been accomplished in dissemination during the present decade, there are still many impediments and obstacles to the dissemination of information. Some of these impediments are briefly summarized as follows:

1. There is the lack of permanent availability of those scientific and technical publications printed by the Government Printing Office; there is inadequate bibliographic control over these publications, and there is dissatisfaction in delays in printing and availability of these publications.

2. There is little incentive to declassify security classified information; there is no requirement for periodic review of security classified information; there is no penalty for overclassifying information.

3. The Export Control and Mutual Security Acts, as variously interpreted by the departments and agencies, are a major deterrent to dissemination.

4. During periods of budgetary restriction there is always a tendency of executive agencies to cut back on oral/informal communications by limiting travel to meetings, telephone conversations, personal communications, face-to-face discussions. This type of communication is vital to information transfer.

5. The Copyright Law is an impediment to the free flow of information. With centralized computerized information banks being set up, copyright is becoming more of a problem as time goes on, rather than less.

6. Proprietary information including trade secrets and certain commercial and financial information must be protected. However, as with all categories of limitations, information

is occasional determined to be proprietary when in fact it should not be so designated, thereby contributing to the overall withholding problem.

REMOTE SHARING OF CLASSIFIED INFORMATION AND PROGRAMS

Bernard Peters, National Security Agency

The existence of computer networks to share data and to act as information and storage retrieval mechanisms raises some questions of interest to the Classification Management Society. Should classified information and programs be entered into such systems? Is it desirable, necessary, possible or avoidable to have classified information of programs in a remote access system?

Is it desirable to have classified information and programs in a remote access system? From a pure security point of view the answer is surely no. Pure security would reduce the amount of classified information which must be protected and would like to protect all that there is as well as is possible. The easiest way to avoid losing classified information is to have none of it. The next is to isolate it in a secure vault which no one opens. However, management's point of view is that classified information programs must be made available on remote access systems, not because this is a status symbol, but because it is necessary.

As a necessity, classified information and programs should be available to remote access systems or the enterprises of the U.S. government and its contractors. These vital programs must be well managed and supported by good computer resources. Some enterprise cases are extremely difficult to accomplish and absolutely require support of major computers. Therefore, classified information and programs must be entered in computers. Because of the difficulty in the generation of programs and data base management, available classified data and programs can only be accessible by remote access computers.

Is it possible to have classified information and programs on computers? The answer has to be yes. So let us now define the problem a little more and say, is it possible to have classified information and programs on a remote access computer in a *secure manner*? Again, I assert the answer is yes. This is not a trivial question, nor an inexpensive question. There is a cost to security as there is a cost to guards, stamps, locks and vaults. There is a cost to security on computers. At times ways ratio of the cost of security for computers seems a little higher than the ratio of other security costs. This may not be true. We will examine this latter.

Is the remote sharing of classified information and programs avoidable? It is avoidable only if we are to deprive the national efforts of the utilization of large data bases and the utilization of large computational capabilities, the advantages of computer managed communications net-

works, the advantages of computers in command and control systems. Because command and control, rocket launch, and other major programs of the armed services are not optional, the remote sharing of classified information and programs is not avoidable.

Does classified information differ from classified programs? In a sense it does, very substantially so. Information is the product and the subject of communications and is protectable with certain relaxations that are important to its management. Some of these characteristics lower the cost and expense of manipulating it. This might be illustrated by considering that a typical message can stand a few letters of garble and still be completely useful to the recipient. Most communicators have already developed a manner of writing which avoids the hazard of completely inverting the meaning of a message. Typical of this is the "not, repeat not" sequence found in certain messages. At this time there has not been a sufficient development or awareness by some of the computer community of the difficulty of suppressing garbles. They rely on large block sum-checks and retransmission. However, there are developments in handling codes and forward error correcting codes which represent a substantial improvement in this area. Information does differ from programs at this time for remote access computers because communicators are more experienced in dealing with information than they are with programs. It is to be expected that the handling programs will reach the same level of excellence as time goes by.

There are several levels on which computers can be remote accessed. The simplest and easiest to manage is an inquiry only system, such as airlines reservation or stock control. Inquiry includes entering material into a data base or retrieving data from it, but in no way altering the available functions to the user. The typical user has a set of specific commands which he can utilize to ask particular questions of the data base. Or he has a set of commands and capabilities for entering or correcting those portions of the data base which he is authorized to manage. Inquiry in this sense is definitely easier to control and manage under a real-time software secure system than is a more general case where the individual may write particular programs to compute or derive answers which he wishes.

The next step in the scale of difficulty for protection is the interpretive system, such as BASIC, JOSS or QUICKTRAN. These systems provide a capability to the individual user to construct a program which will answer specific needs. Such systems take a fair number of functions which are quite general in nature and patch them together to produce a computer sequence which produces the required answers. The programs written under such systems can be quite powerful and derive the full range of material which a general user might want. However, from a computer point of view, interpretive systems are more costly than they need be because of the interpretive requirements. They also lack a generality which could be crucial in plans for later expansion.

The interpretive system can be as secure as any other system, but might be less immune to machine failure

than a more general machine language system which considers the user to be significantly more hostile than does the interpretive system.

The final or most difficult case to manage in a remote access system is the full capability system. Some set of users at some set of terminals may write in any language they choose including machine language. Controlling this requires the construction and management of bounds registers on both data and program. It requires proper control of I/O devices, I/O access, clocks and allocations of the various resources of the computer. This is all accomplished by the monitor. If the monitor is sufficiently secure, it protects the system against debug errors or even more hostile use by an intelligent individual. On most systems, assault on the integrity of the system comes from an improperly debugged program. It seldom comes from hostile agents.

What are the prerequisites for having a secure remote access system which is useful to a specific enterprise?

The management of the enterprise must be aware of the need for security and must see that this security exists. Further, and more difficult to accomplish, the management must be competent, specify what security is desirable, determine what the characteristics of secure operations are, and to judge whether or not the security has been obtained.

Some managements have not considered that there is a threat to the security of the system. There are more than a few threats. An assessment of the threats to the integrity of the data and the system is an important part of the management's responsibility. It is hardly necessary to lean on this as a specification at a meeting of the National Classification Management Society. The Society must be all too aware of the difficulty of impressing line and operation managers of their requirements to recognize security short comings or classification management difficulties.

Difficulty of having competent security officers with an appropriate command overview of the computer system can be very serious. Too many computer systems are operated by a contract software house using subcontract software houses in an open environment with the computer system maintained by vendors. Sometimes this is supplied for a submanagement element which may not even be fully aware of the security of the array of data which is being passed on the computer system. This is very hazardous especially in situations where the operating element for the computer is one that was chosen for the convenience or ease of fiscal responsibility. Comptrollers have a strong understanding of the need to manage the pennies and the dollars. They sometimes fail to understand the technical interplay of various pieces of data. The expertise to make a judgement about whether a software system is secure, or a computer system is secure, consists of more than the ability to write a program, more than the ability to measure whether or not the operators are spending too much time mounting tape, and more than the ability to register jobs in and out. Important judgements must be made and documented about the configuration, the competence of the monitor and the possible breaches of security

which can be caused by failures in the standard operating procedures. The establishment of valid and effective operating procedures is a difficult but absolutely necessary requirement.

Any remote system which utilizes communication lines must have communications lines which are appropriately protected. This can vary from small considerations like the lines should have a great deal of physical integrity, to higher and higher levels of attention, such as authentication system and enciphering systems.

The computer must be operated in a controlled, secure fashion. It is difficult to imagine that one can rent time on a main frame, using someone else's operators, and operate in a secure fashion. It is, therefore, necessary that appropriate contractual or proprietory arrangements be made so that the computer is effectively under the control of the enterprise. Under the effective control of the enterprise may encompass including engineering personnel and maintenance personnel in the operating enterprise. The securing of the computer center extends to many attributes of physical security which are adequately covered by appropriate governmental regulations and literature of the industrial security industry.

For the system to operate satisfactorily, it needs a really secure monitor. The secure executive system controls the computer at all times. Most executive systems are supplied by the manufacturer. In many cases the supplied monitor is not satisfactory for providing security on a National Security level. For many other enterprises, such as banks, insurance companies and airline industries, it would be possible for this monitor to be acceptable. The acceptability of the monitor is a management decision that must be made after a careful analysis and competent study. Secure monitors cannot be assumed for any computer on the market at this date. Specifications for a secure monitor have been made by other papers.

Appropriate work space must be provided for the terminals which utilize the remote access computer. It is certainly not acceptable to have secret material typable or displayable in a space cleared only for confidential. Questions of physical security management, therefore, are of considerable importance. On occasion, people have proposed that we have terminals which are operating principally in open areas. An area cannot be open and contain secure material at the same time subject to arbitrary viewing by unknown persons. The physical security arrangements for the handling of most classified materials will adequately protect the general form of the terminals available.

It is important that appropriate work spaces for the terminals take into consideration the comfort and convenience of the operator. If the space gets too hot he will leave the door open and violate security. It is unreasonable to put a good, loyal, trustworthy and discrete operator in a small airless cubby-hole, with a heat generating terminal that is too noisy and inconsiderate of his feelings.

Personnel selected for operation of the system need not be super-loyal people, nor should they be overly qualified. They should be adequately qualified for the job at hand. They should then be given a standard oper-

ating procedure which is clear and specific on their obligations and responsibilities. Personnel considerations also demand that sufficient attention be given to the question of turnover of systems managers, systems programmers, and audit personnel. The security personnel, the personnel who make the security work, must not be so transient as to turn the whole project into a farce.

There must be an auditing activity. There should be an inspectorate or auditor activity which determines that the minimum security criteria are being met on a daily basis. It is not acceptable to assume that security can be established by doctrine, specification, and even preliminary training without continuous review. Security enforcement is a specific nondelegatable responsibility of the management of the enterprise. There must be a continuous review on the part of the senior manager that auditing is going on and that it is effective and responsible. At times in certain enterprises because the auditing activity has found nothing, it is suggested that auditing should be discontinued or lowered in value or varied. This is not acceptable on the same basis where no one tried to break into the vault that we should only lock it on alternate Thursdays.

It is clear from the prerequisites that certain tests can be made about whether a specific enterprise is or could be secure. A simple test one can make is a test of the chain of command. Is the chain of command specific? Is there a single individual who could walk up to the main frame of the machine, notice that the typewriter is typing out something unacceptable and force that to be changed? This is a physical test. If the machine ordinarily types "error," could it be changed to type "failure" on the command of a single individual who has specific authority to enforce it. If this is not true, there is reason for doubt that there is sufficient strength in the chain of command to guarantee that the machine would operate in a secure fashion. It is strongly felt, by this author, that the situations where the machine is furnished by one vendor and maintained by another, with systems designed by a third, programmed by a fourth and operated by part time students from a graduate school under the auspices of a committee which meets semiannually, cannot ever be considered a secure installation. Security is based on responsibility with authority.

It is easy when stressing the need for strength in the chain of command to give the impression that excessive rigidity is needed. This is not true. Standard operating procedures must provide for exceptional conditions. There are many exceptional conditions where there must be a local authority who can make the exceptions on the spot for immediate performance. The system must continue to meet the requirements of the enterprise which has the computer. There is some concern that the exceptional conditions will be forced by a hostile external threat, solely for the purposes of exploiting the exceptional conditions. This should receive due consideration by the security officer concerned. However, in general, operating computer systems have many difficulties and many exceptional conditions which are beyond the control of both

the owner and the hostile threat to the computer system. These exceptional conditions must be met.

If one is operating a computer system for the United States Government a security stop can say that file X cannot be printed. If the man on the other end requesting file X is the President of the United States, you must have a bypass. If there is not a secure, thought out approach to bypassing that security stop, the machine will arbitrarily be forced to pass all security stops to print out the file. For the owner or commander of the enterprise will have his work done. That is the purpose of the computer. The important concept here is that foresight and provision for override and exception, the bulk or a majority of the security mechanisms can be kept enforced, can aid and support the security. Failure to provide for exceptions, for overrides, and for local authority to act, under logging conditions, if necessary, weakens security, it does not improve it.

Expenditure for security is not unlimited. It must be reasonable and commensurate with the threat. For each enterprise which seeks to operate a secure remote access system, management has the responsibility to state specifically what the threats are.

Further, management must state what is an acceptable rate of failure. It is impossible to state that there never shall be a failure, since this level of performance cannot be conceivably funded for. One must specify the failure rate as one message in ten thousand, one random message in a hundred thousand, or one message in ten. There is some level of performance which is acceptable and the management has the responsibility to spell it out.

In summary, security of classified data in a remote access system, even as in any batch system, will be as good as the management wants it to be, and no better! Management can cause this to be. They must not delude themselves, they must not claim technical competence they do not have. They must not assume that anyone will meet a standard which has not been set and specified. If the management of the enterprise wants security, it will have it at a reasonable price.

PANEL – CLASSIFICATION MANAGEMENT TODAY

Wayne T. Wilcox, Jr., Arinc Research Corporation, Moderator

Wilcox: I felt very honored when Jim Bagley asked me to chair this panel. I couldn't help but remember Howard Maines' comment during the business meeting at San Francisco. He commented that here we are, The National Classification Management Society, but at our Seminars we seem to talk about everything but Classification Management. I'm very proud to be able to introduce this subject to this Society.

Jim gave me a lot of leeway, so it was decided to tackle the subject "Classification Management Today" from the thought "How would you go about selling a classification management program to skeptical management?" In essence we will examine the cost effectiveness of Classification Management in industry.

Let me digress for a moment and put what we are going to talk about in proper perspective. The defense industrial complex has come to use the words "cost effectiveness" with ever increasing disregard as to their meanings. They are used and expressed as two words only because of the disciplines of the English language. Cost effectiveness is not a phrase with a nice, concise, definition. Instead each word must be examined. The effectiveness, or what needs are fulfilled and what benefits are derived from a system, and then what does this system cost? The "effectiveness," or benefits gained, are not necessarily measured in dollars and cents saved. But for the system to be cost effective, the benefits gained must be worth the cost.

Another thing that is going to be a little unique is that we are going to discuss Classification Management, not from our usual approach of the government giving classification guidance to the contractor, but rather what happens in industry after this guidance is received. Believe me, the DD 254 even if it is filled out properly, which it seldom is, is not the final answer. The contractor has to see if he can deduce what the guidance is, and what does it mean to him in the performance of the contract. It is a whole new world, a real world, somewhat removed from the high pronouncements from the hallowed halls of the Puzzle Palace. So with the exception of one presentation on the Naval Material Command, our presentation this morning is all industry and more or less pointed toward industry. Possibly you government types may be interested.

You have the biographical sketches of the Panel Members so I won't waste your time with lengthy introductions. They are all seasoned practitioners of art of Classification Management in Industry. I hope we create a lot of questions and comments, that's our purpose. Please hold your questions until the end, and then we'll do our best to answer them.

Keeping this in mind, let's look to Sylvania Electronics Systems, Mountain View, California, which has a well rounded, functioning Classification Management program and ask J. R. Rasmussen to tell us "What bene-

fits are to be expected from an effective Classification Management program."

J. R. RASMUSSEN

Sylvania Electronic Systems

The Classification Management program at Sylvania Electronic Systems—Western Division became a fact in early June 1966, at top management's direction. The program implementation was left to the Security Department, under which the program operates today. It was necessary at that time to provide our ideas and thoughts for approval and I would like to quote a part of Ken Wilson's response to top management on the subject.

"Classification management programs are too frequently justified on the basis of glittering generalities and inconclusive specifics. It is pointed out that the reduction in classified holdings usually associated with a program which encourages less over-classification and more rapid downgrading will save money— and, if properly supported by management, it is true that some part of the program costs will be recoverable in this fashion. It is further claimed that such a program will lessen the impediments to the exchange of technical information and permit more effective utilization of the engineer's time—and with appropriate co-operation of the technical staff this also can be true. However, three incidents which have occurred in the past month provide graphic examples of a far more cogent reason for a classification management program, i.e., to assist in avoiding mis-classification of information resulting in possible compromise. Such incidents engender a reputation for poor security—or in the current terminology popular with the government agencies, an "unsophisticated" security program. In the defense industry, this can be almost as detrimental to a high level of contractual activity as poor quality or inordinate costs. It is pertinent, therefore, to examine such incidents with a view to eliminating their causes and recurrence.

"The most frequent reasons assigned for an event of this nature are "human error" or carelessness on the part of the originator and "too busy" or "took subordinate's word" at the reviewing level—or "deadline to be met" as applicable to both. There is little question that such an assignation of blame is at least partially correct in most cases. But to rest sole responsibility on this foundation is to make the following assumptions:

"1. The government supplied complete, clear and timely security classification guidance;

"2. If not received concurrently with the RFP, RFQ, or contractual document, immediate steps were taken to obtain such guidance;

"3. When received, it was reviewed in light of the known perimeters of the program to assure its completeness and clarity, as well as to identify any special areas of care that might be foreseen from the conditions imposed;

"4. Any deficiencies, inconsistencies, or questionable restrictions were resolved with the Contracting Officer at once;

"5. When appropriate, a concise summary of the requirements of the

government-supplied guidance was prepared in a standardized company format for ease of reference – along with specific procedures for satisfying any special demands set forth in that guidance;

"6. A copy of the classification guidance was distributed to each member of the technical staff to be associated with the program and to appropriate administrative personnel, e.g., technical editors;

"7. An established procedure existed by which the engineer could obtain information or decisions concerning the interpretation and application of such guidance as well as answers to questions concerning the currency of the classification of documents from which material was to be extracted;

"8. The engineer had available to him a means of ensuring that pertinent classification guidance furnished with respect to the same information under other contracts were consistent with that he possessed, and finally;

"9. There was a provision for review of any document when substantial doubt as to its proper classification existed.

To the extent that any of these assumptions are not valid, the individual must be absolved of a commensurate degree of responsibility."

These nine assumptions that I have quoted, together with the ISM requirement, for extracting and preparing classification guidance for potential and actual sub-contractors form the basis of a Classification Management program.

There are many things to consider in the establishment of a Classification Management program. For example, the number of active classified contracts at any given time and the number of employees within a facility. At Sylvania we regularly manage approximately one-hundred classified contracts from various User Agencies and have around 3,500 employees, 3,000 of whom hold some level of clearance. Our staff consists of a supervisor, three analysts and a secretary. The necessary staffing level of a Classification Management program is varied and could be as numerous as there are companies interested. Such a staffing endeavor could only be established by balancing the risk of too little effort against the cost of too great a program. This would have to be a management decision within your respective facilities. I do have three different classification management staffing suggestions with their respective areas of responsibility. Time does not permit an examination of these; however, I can make them available at a later date to anyone desiring copies.

We have found that a classification management effort in which the responsibilities are divided among several different functional units of a company, suffers greatly. The responsibilities are usually handled by a contract administrator, a sub-contract administrator, a program manager or some other technical staff member, usually resulting in the classification management effort being only a sideline to the main responsibilities of the individual involved. Being a sideline, the responsibilities fall by the wayside and in many instances are not completely accomplished when they

should be. We have also heard that small contracts or small proposals do not require as much attention as some of the larger efforts. We believe this to be a false assumption. There can be as many or more security problems, hence Classification Management problems, existent in small contracts as there are in large contracts. We feel it is therefore important that a single administrative entity be responsible for the entire Classification Management function. Much has been said, and there have been debates on just where this responsibility should lie within a facility. We feel the responsibility lies within the Security department, due to the liaison within the various groups that is necessary in accomplishing our functions. Regardless of its location, a most important point is management's understanding that this unit, must of necessity, have a broad span of contact with both the technical staff of the company and the classification personnel of the various customers. This important point is well established at Sylvania, Classification Management being the prime point of contact with any and all user agency customers on classification problems, or classification resolutions. We would envision the qualifications of classification personnel to consist of a professional level type person. with education and/or experience in a technical field as well as a certain amount of administrative responsibility in his background, and we would prefer industrial security experience.

Classification management is recognized and endorsed by the Department of Defense. To this end they are taking steps to establish Classification Management personnel within the various user agencies more and more. As you know, it was not only the government that recognized the need for a Classification Management program. NCMS was founded by a group of forward looking personnel who were involved in security and classification work, both in industry and governmental agencies. The various user agencies are requesting more and more contractor support in making recommendations for improvements in their directives and security guidance. Classification management, as a function, is a new idea to most organizations. Traditionally, both policy and operations for the simple aspects of classification management, have been performed or ignored by various functions. The value of a well-rounded program in both increased security protection and reduced cost, is an established fact. We will hear later on from the other panel members concerning cost savings aspects of classification management. I would like to tell you a little war story that actually happened at our facility.

We had received a small contract which called for a certain type of antenna to be mated with and tested on a missile at a remote, mountainous test site. The security guidance we received specified that the missile and our antenna would be classified confidential. The contract was for some three months duration and less than $50,000 were involved. In reviewing the guidance we received, we found that what was actually classified about this effort was only the method of mounting the antenna on the missile and our test

results. This was confirmed by the contracting officer. It was further suggested that the missile be stripped of all components, thus allowing shipment and receipt of only the case which was unclassified. A recommended DD 254 was submitted which was subsequently approved and returned to us as our guidance on the contract. The contract was later completed without the need for 24-hour guard service at the test site and resulted in an accepted cost savings of just over $8,000.

Similar cost savings, although not always available in tangible dollar amounts, are available to the professional classification management man in performing his daily functions.

The point of this little story is that had we not been in existence, it is very probable that a 24-hour guard service would have been mounted, and we would have realized a contract overrun amounting to at least $8,000.

I would say that the prime objective of a company Classification Management program would be to insure as much as possible, that all material generated in connection with classified government contracts is correctly classified. I emphasize "correctly" because under-classification and over-classification are equally grave sins. Over-classification, of course, causes wasted motion and unnecessary cost, and consistent over-classification also serves to degrade the effectiveness and integrity of the classification system. Under-classification, of course, could lead to compromise of information, costly investigations, and other time consuming actions necessary to recover and upgrade documents.

The secondary objective of a company Classification Management program, should include cost reduction, free dissemination of legitimately unclassified technical and scientific data, and increased respect for the classification system and the security program.

There are several specific classification functions which we consider essential to an effective program. I am going to discuss them in the same order that they would be encountered in initially establishing a program.

1. Interpretation of Customer Classification Requirements. Analyze the security guidance, the DD form 254, as received from the user agency. Make your interpretation in conjunction with the technical staff, if necessary, and above all insure that security guidance is received if the effort is classified.

2. Preparation of Guidance for Employees. After the DD form 254 interpretation process, the next logical step is preparation of internal guidance for the technical staff who will be associated with the contractual effort. Publication of such a comprehensive company guidance, will provide a common interpretation for each person who has need for the information, and you are giving your employees the detail they need, in the language they understand.

3. Employee Education. This step is important to a Classification Management program. If employees do not understand how to use the guidance the specialist has prepared, he has wasted his time. We recommend all possible means of education be utilized, to pass this information on to

those who will be working with the classified programs. We also recommend an extensive education program, with the contract administrators, proposal and contract managers, and the sub-contract administrators during the initiation phase of a new classification management program. This education should be constant and continuing.

4. Preparation of Guidance for Sub-Contractors. A large majority of contractors prepare the DD 254's for classified sub-contracts in accordance with the ISM. The considerations in preparing the DD 254 for sub-contractors are the same as for preparing guidance for your own employees. The majority of anticipated questions should be answered in the DD 254 and the revisions made as often as necessary. Superfluous material should be avoided, and the 254 should be tailored to the specific sub-contract effort.

5. Reviewing Material for Correct Classification. This is an area of activity which can be extremely beneficial. It would be desirable to find methods for systematically reviewing the entire inventory of classified material, beginning with the oldest material on hand. Such review can be lucrative. As one company reported, they had removed over 20,000 secret documents from their system inventory, as a result of downgrading actions.

The second aspect of classification review concerns material currently being generated. The main thing here is to establish workable avenues so that classification specialists are available to assist employees at arriving at their classification decisions. It is in this phase of the program that the need for knowledgeable personnel is most apparent. The Classification Management specialist must be able to grasp and understand the rudiments of technical data and he must be able to converse fluently with members of the technical staff and ask them sensible questions.

Another function of the classification program is review of customer classification requirements. By this, I mean the periodic review of DD 254's for both current and completed contracts. For example, the very nature of a complex R & D contract makes it difficult for the customer to initially define precise classification requirements for the entire technical scope of the project, which may stretch for years in the future. At the offset, there sometimes isn't even a clear picture of what the end item will be; so as the project begins to take shape there may be many areas where the initial customer classification guidance becomes inadequate or needs expansion. State of the art advances are another reason why reviews are necessary. When periodic reviews of DD 254's indicate changes in classification are warranted, recommendations should be documented and forwarded to the customer.

In the area of release of information for public dissemination, it is highly recommended that Classification Management review each and all items of information intended for public release, and make recommendations and suggestions as to where the material must be forwarded for official DOD approval.

In summation, then, a Classification Management Program will:

- Cost Money, without a doubt.
- Recoup some of this investment through reduction of over-classification and establishment of a document reduction program.
- Materially assist in avoiding security incidents resulting in under-classification.
- Provide a co-ordinating point at which the guidance from the government and the classification efforts of the engineer can be sure of meeting.

These items are the benefits that were achieved at Sylvania and can be expected from an effective Classification Management program.

To quote Ken Wilson again: "Within the range of economic feasibility, and human fallibility, the program can neither guarantee review of every document produced under classified contracts nor 100% accuracy in the results of the classification effort." However, I believe that an established Classification Management program is a definite advantage and asset to your company employees, your company management, and to your facility.

Wilcox: Thank you, J. R. I think we have just been given a pretty good insight as to just what management can expect from a good Classification Management program. I would like to emphasize some of the points J. R. made:

1. The prime objective of a company Classification Management program is to insure as much as possible, that all material generated in connection with classified government contracts is correctly classified. Emphasis on the word "correctly".

2. A good company Classification Management program will materially assist in avoiding security incidents resulting from under-classification, and

3. It will cost the company money, without a doubt.

As was stated, a contractor can do very little in Classification Management unless the government, User Agency, if you will, supplies the contractor with complete, clear and timely security classification guidance. George MacClain and his co-workers have provided us with a new and revised DD 254 which, I think we'll all agree, has been a step in the right direction. We now have a vehicle for this classification guidance that when properly completed helps a lot. The Air Force and the Army have established and fairly well publicized their Classification Management programs and the organizations to support them. But, at least to me, the Navy has been somewhat of an enigma. So when I was putting this panel together I asked Bob Green of the Naval Material Command Headquarters if he would care to shed some light on just what the Naval Material Command was doing in the area of a Classification Management program.

So next to talk to us is Bob Green, Head, Classification Management Section, and Senior Assistant in the Security Programs Branch, Headquarters, Naval Material Command, who will shed some illumination on Classification Management in the Naval Material Command.

R. E. GREEN
Naval Material Command

In recent months I have heard a number of remarks to the effect that the Department of the Navy Classification Management program is the best kept secret of our times. It has even been suggested that it does not exist. We may be guilty of not giving the program the right kind of exposure; but, as many NCMS members can attest, there is a program underway and it is increasing in its impact and effectiveness. When the panel chairman invited me to speak on this subject, I welcomed the opportunity to dispel what has been called "the Navy enigma," subtitled "The Silent Service." Before proceeding, let me make it clear that I am not a spokesman for the entire Department of the Navy Classification Management program. That responsibility rests with the Office of the Chief of Naval Operations, ably represented by our fellow NCMS member, Dan Rankin. I can speak for the Naval Material Command which is comprised of the six Naval Systems Commands the Navy Research and Development Laboratories and Centers and, in total, some 300 subordinate activities, employing nearly 300,000 personnel, with the major function of developing, producing and maintaining the material needs of the Navy operating forces. A recent survey identified some 354 weapons systems currently in RDT & E under the cognizance of the Chief of Naval Material which have a total acquisition cost of $52 billion and an estimated life cycle cost of $360 billion. The projects, contracts and sub-contracts which support this effort number in the thousands. On that basis, I think it is safe to say that, as a Command, we generate a major portion of Navy classified information.

It follows that we should be generating a major portion of Navy classification guidance. In the next few minutes I will describe the NMC concept of Classification Management; how it works; where we think we are today and where we hope to go.

The principles and objectives of the NMC program are identical to those of other DOD and industry programs and we won't belabor them for this knowledgeable audience. Since the contention has been made that the Navy CM program is somewhat obscure, a brief outline of the basic Navy CM organization seems to be in order. Responsibility for developing Navy policy in support of the Department of Defense requirements is assigned to the Assistant Chief of Naval Operations, Intelligence, Security Policy Branch (OP-92C2). The basic Navy directive establishing a formal CM program was issued in 1964. It was followed, in 1965, by extensive changes in Navy security regulations designed to implement the program objectives. One of the key features in these procedures assigned the total responsibility for the CM program to the individual in each command designated as the activity Classified Material Control Office (CMCO). This is a mandatory billet in every Navy command and therefore, automatically establishes a point of contact for CM matters. As the organization title implies, OP-92C2 is responsible for security policy for the entire Department of the Navy.

Within the Office of the Chief of Naval Operations, Classification Management is an operational function of the Director, Administrative Services Division, OP-09B2, who is the designated Classified Material Control Officer. This office has a critical role in insuring the success of CM programs throughout the Navy; since the basic security classification guidance for Navy projects must be issued by CNO as a part of formal planning and requirements documents such as the SOR, TSOR, GOR, ADO and others. All other detailed guidance issued at any phase of development, production or operational use derives from this basic guidance.

At the time the formal Department of the Navy CM program was set in motion, the Material Commands were undergoing a major reorganization which saw the Office of Naval Material/Material Bureaus concept abandoned in favor of the single Naval Material Command. This was accomplished through several phases during 1965 and 1966 and the reorganization effort resulted in a number of new program efforts being delayed. Thus it was not until July 1967 that the NMC Classification Management program was born. Although exercised at a different level of organization, the same division of policy and operations found in the CNO program exists in NMC program. The security Programs Branch (MAT 0522) is a part of the Naval Material Command Headquarters organization and, like CNO, provides policy guidance and monitors the total security program for the entire Naval Material Command. This office is involved in the operational aspects of Classification Management — that is the development and issuance of guidance for specific projects — only when technical cognizance of a project is retained by the Headquarters, CNM. Otherwise, the operational functions of the program are exercised by the Systems Commands, Laboratories, and Centers assigned as the principal development activity for each project.

Our concept of operations is simplicity itself and consists of just four points:

1. Every activity in the NMC involved in classified projects will have a formal CM program.

2. Every activity with a formal program will assign responsibility to one individual or office to speak for the Command in CM matters. In keeping with Navy security regulations this is the activity CMCO or a specifically designated classification manager who reports to him.

3. Every activity will receive or will obtain classification guidance for every classified task assigned by higher authority and will furnish guidance with every task assigned by them to other government or industry facilities.

4. Every activity will continue to provide current guidance for the life-cycle of each task assigned. This may involve initial development and production only or it may extend into fleet operational use and ultimate disposal of systems and equipment.

We recognize that the Naval Material Command is technically oriented and that our input to the classification decision must be limited to technical

matters. When security classification of information must be based on other considerations outside of the cognizance of the CNM, such as long range requirements, plans and objectives and actual or planned fleet operational employment of hardware, the originator of the task must provide adequate guidance in the tasking document. As the first step in our program, NMC classification managers are currently examining old and new task assignments to insure that adequate guidance has been furnished. When it has not, they are actively seeking more information from the task originator. Ideally, this takes place before actual start of work, so that we don't compromise a project through lack of communication. On old tasks which are well down-stream and on which a classification pattern has formed despite a lack of initial guidance, we attempt to confirm what we are doing in the hope that if we are in error, something can be salvaged, security-wise or cost-wise. This first step defines the workload and provides an authoritative basis on which to proceed.

With the incoming tasks identified, the classification manager, working closely with the technical project manager, insures that the guidance contained in the tasking document is made available to everyone involved in the effort. At this point the CM and the technical project manager determine what additional, more detailed guidance can be given to relate the basic guidance to the specific work elements, equipments and components which can be identified at this early stage of development. The guidance which results from this joint effort becomes a part of the master plan for the project. In the formal Navy planning documents cycle these are referred to as TDPs (Technical Development Plans) and PMPs (Project Master Plans). The guidance contained in most TDPs and PMPs is generally adequate for the initial study effort, whether conducted in house or contracted out to industry. In the latter case the classification requirements of the TDP or PMP are incorporated in the mandatory DD Form 254, Contract Security Classification Specification. When a total RDT & E effort is to be performed within the Navy or DOD, a separate Navy directive may be issued to supplement the TDP/PMP guidance. In the case of full scale RDT & E or production contracts, a concerted effort is being made to provide as much detailed, narrative classification guidance as is available, rather than to rely on the out-moded check-list approach. I feel that individually and as a group, NCMS members and friends have heard more than enough about the merits and evils of the DD 254. I do not intend to pursue the subject except to say that NMC activities are required and will try to give industry the most detailed guidance possible with every task involving access to classified information. If we fail through oversight, negligence or lack of information, you are invited to take us to task so that we may improve.

Before moving on to another phase of the program, there is one other form of guidance I would like to discuss very briefly. One of the justifiable

complaints of industry concerns inconsistencies in classification of identical or similar information by the Air Force, Army, and Navy and frequently by commands of the same service. The problems created by this situation are self-evident. The solution lies in a much greater degree of coordination within the DOD to insure that, to the maximum extent possible, information having multi-agency interest and common applicability, is consistently classified. The tool by which this is accomplished is what I call a DOD or Joint Agency Subject Matter Classification Guide. There are a number of such guides in existence on subjects such as thermal batteries, lasers, infrared photography, night vision devices, nuclear weapons and others. In time there will be many more as common areas are identified and agreement is reached on levels of classification. This effort is being "honcho-ed" by our NCMS friends, George MacClain and Don Garrett of the Directorate for Classification Management, OASD. I know they won't mind if I suggest that you contact them if you know of a subject which might be a candidate for a DOD subject matter guide.

Another key point in the NMC concept concerns the authority to approve, issue, and interpret classification guidance. Within activities of the NMC this responsibility is centralized in the CM organization. This does not imply that the CM is almighty. He cannot and does not operate in isolation. Every decision reached for the command results from a coordinated review by the technical side of the house, contracting officers, public affairs officers and security officers. But someone must coordinate, mold opinions and decide — someone must answer authoritatively for the command. This is the role of the CM in the NMC. Under this concept, all guidance issued by the command in any form, including the DD 254, must have either the approval of or the signature of the CM and all inquiries should be directed to him.

If I may digress for a moment, I began by saying I hope to give exposure to the NMC program. As partial proof that it does exist and to help you find your way around, a roster has been compiled, listing classification managers in the major NMC commands responsible for technical developments. A copy of this roster is included in the program material distributed before the opening of this panel.

When the best guidance possible has been developed, there remains the problem of getting it to the user and keeping it current. In this respect the NMC program has no novel approach to suggest. We classify security guidance in extreme cases only, thereby permitting and encouraging wide dissemination. We require that guidance be reviewed at every change of development phase and at least annually. These reviews are conducted in the same channel as the original classification decision and are similarly coordinated and controlled by the CM.

From the foregoing, you can see that the NMC has a well-founded program; but that alone does not spell success. I, personally, cannot assure this Seminar that the program is meeting its objective today; that it will tomorrow or next year. It is fraught with complications, inadequacies and un-

explored problems. But, compared to yesterday (1967), when we had nothing but a token program and didn't truly understand that, we have started to move. Today, (1969) we have organization, policy and procedure. Because of our persistence, we have some initial guidance where previously we had none. We are developing subjective guides for use within the Navy and contributing to those developed by DOD. Every classified development plan and contract has a classification guide. Tomorrow (1971 or earlier) we hope to significantly improve the quantity and quality of guidance, to provide more timely and meaningful review and to take much more positive actions to declassify the mountain of classified material we have created and left behind.

These are goals we expect to meet. There are others which are more difficult to solve and which, looking squarely at the facts of life, may never be adequately solved. These are our real problems and therefore our top priority goals. At the top of the list, as always, is resources: obtaining adequate numbers of people to manage the monstrous workload we are uncovering and training both classification specialists and other administrative and technical personnel in CM techniques and procedures. An underlying problem in this program is the lack of adequate numbers of experienced classification specialists. It is a strange and sad commentary that after so many years of classifying information, our approach has been so dis-organized that we have relatively few qualified specialists. As a result we must hire on potential and provide the training. Naturally, first year production suffers greatly. The few specialists available today must spend an excessive amount of time educating those with whom they must coordinate and production suffers again. There is also the problem of educating management to the need for and advantages of CM. We cannot sell this Program on the mandatory requirements alone. Management understands dollars and cents. As we all know, factual cost savings and cost reductions have been extremely difficult to identify and substantiate and yet it is on this basis that we stand the best chance of really selling the program. My personal feeling is that we must establish a set of benchmarks in both government and industry, as realistic as our current experience will permit, to determine what security is costing us today. Only on that basis can we judge the effect and value of the CM Program. To be meaningful, any benchmarks we adopt must be broad-based rather than on individual activity findings, thus a cooperative DOD/Industry venture is clearly indicated.

We hope, in time, to establish earlier and closer liaison between NMC classification managers and their industry counterparts for the purpose of developing contract security classification specifications which are thoroughly realistic and understood for both bidding and performance purposes. Ideally this would involve pre-contract and post-award security conferences for all classified procurements, but particularly those involving research studies and RDT &

E. The list of goals is endless it seems; but one more must be mentioned. We have just begun to identify the tremendous workload in classification management in the NMC. Under present and projected manpower restraints, that workload will surely defeat us unless some of the more routine functions can be automated. Such items as annual reviews of guidance, downgrading and declassification actions, retention authorities, and even standard classification patterns are possible candidates for automation. We have addressed this area only as a possibility. A great deal more serious thought and hard work are in store before it will be a reality.

These are our problems and our goals. We recognize that they are not unattainable or unique and that, in time, they will be solved: if not by us, perhaps by you in a way we can all utilize. With this for background, I hope that any "Doubting Thomas" is now convinced that the Naval Material Command is very much in the CM program. In a sense there is only one program and we are all a part of it, government and industry alike. We all have guidance to give and we all need guidance to insure that necessary security requirements are met. By working together in closer day-to-day relationship and through such professional groups as the NCMS, we can improve our skills and we can achieve the goals we have set. If the CM program had a watch-word, I think it would be "challenge;" for each of us must challenge every individual decision to classify with intelligent and purposeful questions and each of us must accept the challenge this program offers to contribute to the welfare and security of our company, our agency and our Nation.

Wilcox: I thought that presentation shed a lot of illumination on classification guidance within the Naval Material Command. I know the roster of classification managers in the major Naval Material Commands is going to be a big help to all Navy contractors.

I have been struck by the recurring theme contained in J. R.'s presentation and then again in Bob's. This is, Classification Management is not an end unto itself and it can not be done in isolation. I wonder how many otherwise good programs have foundered because this point was missed or ignored. The classification manager, or whatever title he has, has to be a member in good standing of the team performing on the contract. And he can't be made a member of the team too early. During the proposal concept formulation he is as valuable then as he is when you get down to arguments over paragraph marking of the final report delivered on the contract. I think Virgil Herald, General Precision, Inc., Glendale, California, points this up very strongly in C/M Case Book Number 3 which was just distributed with the C/M Bulletin and is available in the North Room at this Seminar. You people that think you shouldn't rock the boat on a proposal because the government might consider you non-responsible ought to take GPI's experience to heart. We are a team, government and industry, and neither of us is so all-knowing that we

can get along without the other. And this is specially true in the field of Classification Management.

To go on with our presentation, let's see if we can identify one other aspect of cost effectiveness of Classification Management, namely, *costs*. I have asked Dick Boberg, of Aerospace Corporation and our newly elected President, to examine the cost considerations of Classification Management.

RICHARD J. BOBERG

Aerospace Corporation

I think I should begin my portion of the program by advising you of what I am *not* going to tell you today. It will not be a review of the results of a statistical study. It will not result in a neat and concise formula for the solution of any problem. I will offer no panacea — perhaps not even an answer.

What I do hope to do in the next few minutes is to share with you some of the concepts and thoughts that came to me as I was reviewing the subject. Most importantly, I want to stimulate your thinking about this subject and hopefully rearrange your prejudices so to speak in regard to the costs of your classification program.

Several months ago when Wayne asked that I appear on this panel and take on the subject of the cost of classification, it occurred to me that virtually nothing has been said or written, at least publicly, on the specific subject of the real costs of Classification Management. Most all of the presentations and papers given in the past have spoken in glowing terms of the *cost savings* or *cost avoidance* inherent in a Classification Management program. This includes, I must confess, my own presentation to management a number of years ago in presenting our own program.

Now I mean no offense to those who have used this approach because I suspect that many of us have never determined what the real costs of a good Classification Management program are.

Even if we have, the reasons the subject has not had more publicity are rather clear.

One — no one, to my knowledge, has been able to sell a Classification Management program anywhere by dwelling on *just* the costs of that program, and two — because I have found that it is most difficult to define, to the satisfaction of all of us, just which costs are attributable only to Classification Management and which should properly belong to security, contract administration, or perhaps simply chalked up as a general cost of doing business.

I thought that I might obtain a set of realistic ideas about this cost thing by writing a letter to a number of my contemporaries in which I asked for information in three basic areas:

1. What costs should be included when we talk about the costs of classification management?
2. What is the nature of these costs at your corporation?
3. How do these costs relate to the cost savings the program is able to provide?

I would like to share with you some of the results of my inquiry.

Probably the most striking responses were to the first question regarding what costs should properly be attributable to Classification Management. I say the responses were striking because I found in them, on the one hand, that at some facilities Classification Management costs, according to the reply, are non-existent because they simply have no program. On the other hand, more than one of the responses indicated that properly, virtually all of the costs normally attributed to an industrial security program including combination locks, safes, salaries for guards, vault construction costs – the entire program – should be included in the cost of Classification Management.

Now we can speculate and even argue as to which of these views is the correct one, or if perhaps the proper position should be somewhere in the middle of the two, but I accepted the fact that in a sense they are both right.

To say that only the direct salary of the Classification Management representative or the person doing that type of work should be included, can be justified in that this is the only cost that often can clearly be defined in a budgetary sense as an "extra" one when comparing a company with such a position as against one without. At the same time, there should be little argument certainly among this group that classification, in a way, is the "mother" of security – though perhaps unwillingly so – in that were it not for the fact that classification markings are placed on a document, none of the costs of protecting, accounting for, or safeguarding that document would arise.

As for question two, dealing with the nature of these costs, I found – not surprisingly – that the dollar figures given were in proportion to the responses to the first question. For instance, if the decision was that the only cost of classification management is one classification management analyst, the total program cost was his annual loaded salary.

Conversely, if my correspondent decided that the costs should properly include essentially all of the costs of dealing with classified material, the total true Classification Management costs were stated as totaling as much as five times the salary of the Classification Management analyst or analysts on board.

It was in going over the responses to the third question, that of relating the costs of Classification Management to the savings provided by the program, that finally a vague form began to take shape for me.

A number of the replies told me that they really couldn't respond to this question in a meaningful way because they have never really considered the cost aspects and could not really relate the two, but that they would be delighted to tell me of the cost savings that had been chalked up over the years.

One fellow told me on the phone that their program had been sold strictly on the basis of the concept that Classification Management does not cost, it pays, and anyone with any sense would forget about the cost aspects altogether.

It was while thinking over all of

these comments and responses that I believe the message that all of these people were giving me, whether they knew it or not, started to come through. J. R. Rasmussen, in the presentation you enjoyed earlier on this panel, gave us the basis for it. He stated, if you will recall:

"The necessary staffing level of a Classification Management program is varied and could be as numerous as there are companies interested. Such a staffing endeavor could only be established by balancing the risk of too little effort against the cost of too great a program."

In order to make my point, I'd like to paraphrase that to state that the staffing of a Classification Management function can only be justified by balancing the *cost* of too little effort against the cost of too great a program. You see, I think there is a point here that I had missed up to this stage and that is this: *Classification Management has a very real cost,* whether you have a program, or, to paraphrase a soft drink advertisement, an "unprogram".

Do you suppose that the firm that has no Classification Management program and no one performing the function has no cost in this area? I think not. Their costs merely take a different form. What of the costs of issuing documents as secret because the author wasn't sure – when the information in reality is unclassified? What of the cost of building a closed area to house the manufacture of a piece of unclassified hardware that is thought to be classified simply because no one gave the subject much attention? What of the costs of tracking down and upgrading documents that were originated with an incorrect classification, together with the investigative costs to determine whether or not there was unauthorized access? This is not to speak of the sometimes indirect but very real costs to the government in changing some aspects of a project to minimize the damage done as a result of a compromise.

Additionally, as has been emphasized from this lectern on a number of occasions these past several days, there are very real costs in terms of "re-inventing the wheel" whenever information which should be disseminated is not because of the "unprogram" approach. My observation has indicated that this results from the fact that the people involved don't know enough about what can and cannot be released – and hence *nothing* is.

All of these I would characterize as the firefighting costs of classification. Whether or not they are in your budget, if you do not have a Classification Management program, or have a meaningless one, they are with you in some quantity. Basic to a good classification management program is the dissemination to all those in your facility who need it meaningful and timely guidance *that is understood.* This, along with all the other proper functions of a Classification Management program mentioned by my fellow panelists, cannot come about by accident. The unprogram will never pull it off no matter how hard you wish it could, and the result of these functions being ignored can generate

firefighting costs for the life of your contract, and then some. If you don't choose to apply the costs to manage these functions, you must be prepared to pay the very real costs of not managing them.

I submit to you, ladies and gentlemen, there are in reality two costs of classification — the formal program cost, and the firefighting cost — and each and every contractor with one or more classified contracts has one or both in varying proportions.

While there are many ways to describe a situation that will create these costs, I think there are three that will demonstrate the point. The first is through a formal program utilizing one or more trained professional classification specialists who properly perform all of the functions that have been discussed here today. The classification costs in this example should be essentially limited to only the loaded salaries of these mentioned personnel.

The second is where we find a somewhat less formal program utilizing, for instance, an industrial security specialist, a contract administrator, or some other employee who is not a Classification Management specialist who can hopefully — while wearing his several hats — get all or at least the most important of the Classification Management functions accomplished. The costs of classification in this instance can ideally be, like the first example, only the portion of this man's time spent on Classification Management — but often must include sizeable firefighting costs.

The third example is the "let the chips fall where they may" approach, or as we have called it earlier, the "unprogram," where no one has really taken hold of the responsibility for the classification functions. In this example, of course, all of the costs are for firefighting.

The choice then is yours, and that of your management. The costs are in reality there, it is just a question of how you want to divide them up.

In closing, I would like to expand some on a thought that my good friend Virgil Herald recently shared with me. Classification Management is a subject not be neatly carved and put on display as having a definite shape and form. It is something like virtue. Most of us admit it has value, but its application is varied according to concept and situation. And is virtue a profitable trait, or is it a costly one? Only you can decide that.

Wilcox: All I can do is echo and reinforce what Dick has said. Government security costs money. It is a penalty we have to pay if we are going to be government contractors and feed at the public trough. Classification Management is a very necessary part of the overall Security program and the investment of funds, or the expenditure of funds has got to be there if you want to continue getting government contracts and keep your facility clearance.

As you know, Dick is with the Aerospace Corporation which is primarily a paper mill, not a hardware producer. I also come from a paper mill, although we are quite a bit smaller. Spectacular, identifiable cost savings

or cost avoidances are real hard to come by in a paper mill. However, there are areas that common sense points you to that helps keep down the overall costs. For example, keep the inventory of your classified documents down. Filing cabinets and locks cost money. Also critically examine your classified reports while they are in the preparation stage. Despite the uproar over paragraph marking, this is one of the better classification management actions that has occurred. Remember our purpose is to correctly classify, not just classify. So this makes our authors identify, to some degree, exactly what is classified in the report. Many times you will find there is very little that is classified in the report. Sometimes, when this happens, the author will discover that he doesn't even need this classified information to meet the objectives of his report. Or if the classified information is required, once in a while you can wind up with a much smaller classified supplement. The cost savings, or cost avoidance is obvious.

It is in the area of hardware production that spectacular cost savings can be made by intelligent classification management actions. One such company where documented savings have been made is the General Electric ReEntry Systems at Philadelphia. So I have asked Charlie Uhland of G.E. ReEntry and Environmental Systems Division to tell us about cost savings achieved through Classification Management in a hardware oriented company.

CHARLES V. UHLAND

General Electric Reentry and Environmental Systems

This will not be an "I did this" or "We did that" type of thing. I refer you to Classification Management's "Casebook CM-1 (10-68)." This will give you all the specifics you need in an actual case history of this type of operation.

This presentation is not meant to teach you anything. It is given to you to remind you of the things you already know about classification management, and to suggest how you can apply that knowledge in your search for cost savings. If you should learn anything in the next fifteen or twenty minutes, let me assure you, it will be strictly coincidental, and I refuse to be held responsible.

In a hardware-oriented company, the sections to concentrate on in considering possible cost savings are as follows:

1. Engineering Design Tracings
2. Manufacturing and Quality Control Tool Design Tracings.
3. Manufacturing and Quality Control Tooling
4. Procurement and Manufacture of Hardware

The normal idea about classifying drawings is that if the hardware manufactured from the drawing is classified, then the drawing must be classified.

Let me borrow a statement from Classification Management's "Casebook CM-1 (10-68)": "A document should be classified on the basis of its own content and not necessarily on its relationship to something else."

It is information and only information that is classified. Documents and hardware are protected because they either contain classified information, or classified information can be deduced from having access to them.

See? I told you that you weren't going to learn anything!

So, you and I understand about information being the only thing that is classified; but mostly management doesn't, mostly engineering, design, planning, tooling, quality control, and manufacturing don't. And, sad to relate, many of the government people who oversee our contracts at the working level do not understand this.

Now, if no classified information can be elicited or deduced from a drawing, then the drawing should not be classified — regardless of the classification of the hardware manufactured from it.

Before we go any further, let me give you one big fat word of warning! If classified hardware is to be manufactured from an unclassified drawing, be sure to mark the drawing accordingly.

At General Electric Re-entry and Environmental Systems Division, we use one of the following type markings on our tracings:

This Drawing Is Unclassified

CAUTION

Hardware Manufactured From This Drawing Must Be Classified

CONFIDENTIAL
Restricted Data

This Drawing Is Unclassified

CAUTION

Hardware Manufactured From This Drawing Must Be Classified

SECRET

These "stampats" are placed directly above the title block of the tracing, at approximately the same spot that the "Title 18" or the "Atomic Energy Act" stamp would go if the tracing were classified.

Assembly drawings hardly ever have to be classified. Where one or more of the assembled parts are classified, however, the above stampat, corresponding to the highest classified part, must be affixed to the tracing.

On tool designs, let's suppose there would be a pattern of maybe 20 holes that was classified, out of a total of 100 holes to be drilled into a part from the tool. The 80 unclassified holes would be located on one sheet (unclassified), and the classified pattern of 20 holes would be located with a list of coordinates on a second sheet. This second sheet could be a size 8½-inch by 11-inch sheet (classified).

When the actual tool is made, it would be unclassified and would contain only the 80 unclassified holes. An additional plate would be made containing the classified pattern of 20 holes, and this plate would be classified. The unclassified part of the tool would have provisions for mounting, positioning, and pinning the classified plate for drilling the classified 20-hole pattern in the part.

This would save in two ways: First, only the small plate with the 20-hole pattern would be classified, so the classified storage space would be much smaller than if the whole tool was classified. Second, the hardware itself could be manufactured and the 80 unclassified holes drilled; it could be handled and stored in an unclassified fashion. In fact, the part could be manufactured up to this point by an uncleared vendor. The part would not become classified until the final 20 (classified pattern) holes were drilled.

There would be less classified storage for the tool, more unclassified handling and storage for the part. And, only one sheet of the tracing would be classified.

This two-part tooling (one part classified and one part unclassified) can apply to inspection tools and designs as well as manufacturing.

This type of application of classification principles is best known — and almost only known — to the classification team. Tangible savings in the hundreds of thousands of dollars have been instituted at General Electric Re-entry and Environmental Systems Division by the practical application of these principles.

From here on in, I'll be pointing my remarks towards the "one-man gang" type of Classification Management. The well-organized Classification Management set-up, with the team concept for each program, would have a representative from engineering, quality control, manufacturing, etc., as part of the team, each with the classification educational responsibility in his own area. The following is for the poor "no team" guys who have to do it all themselves.

The knowledge you possess will help nobody, unless you educate and motivate the key people who must be involved in the implementation of these principles.

For example, be sure the key engineering personnel are briefed on the how, when, and why of classification, and how they can avoid premature and needless classification. Next, the key designers and design checkers must be indoctrinated; then, the manufacturing and quality control tool designers and planners; and finally, production control or procurement personnel, according to your company's system. In the case of manufacturing planning, especially, be sure the planner knows exactly where, in the process of manufacturing, the part or assembly becomes classified. His planning will tell manufacturing and quality control personnel the exact moment the red tag must be applied to the hardware and security measures put into effect.

I would like to conclude with a few items to remember from Classification Management's "Casebook CM-1 (10-68):"

- Do review and analyze each Engineering tracing to determine if classification is required.
- Do not include classified data or measurements which are not essential on a particular tracing.
- Do restrict the inclusion of classified information to as few detailed tracings as possible.
- Do include "flags" on all classified tracings to show exactly what

information is classified.

• Do eliminate any association problems that will result in classified procurement activity.

It is most important to get the interest and cooperation of the key people involved. Without such interest and cooperation, Classification Management can hope to operate at only about 40 percent efficiency.

Classification Management involves specialized knowledge and the ability to educate, interest, convince, and persuade or motivate key personnel in other areas to involve themselves in the classification area of their particular responsibilities; and by so doing, save the company a lot of money.

The key word is *persuade* or *motivate*. Perhaps you will ask: "How do you persuade someone to do something?" In the classification area, everything is done a little differently — a little more concentrated, a little more distilled. To persuade or motivate someone, I advise the "velvet touch," the "soft sell." Let me give you an example: A well dressed gentleman was strolling down a dimly lighted street when a rather bedraggled stranger stepped out of the shadows, touched the gentleman on the arm, and said: "Pardon me, sir, but would you please help an unfortunate fellow who is hungry and out of a job? All I have in the world is this gun!" That is a classic classification velvet touch.

How do you pick out your "key men"? It's easier than you might think. Wander around among the people in each concerned area and get talking to a few in each area. Pick the ones who are happy doing their work and who show pride in their job. Show a man of this type how to do his job better, and you can be sure that he'll do it better. And, you can be just as sure that he'll contact you to solve any problems that may arise involving classification.

Once the classification man has picked his key men and indoctrinated them into the mysteries of classification, he must have faith that they will handle the classification responsibilities in their particular job.

So, have faith, and, with your special knowledge, go out and educate, interest, convince, persuade, motivate — and save your company a lot of money.

INTERAGENCY LIAISON ON CLASSIFICATION MATTERS

General Jacob E. Smart, USAF (Ret.)
National Aeronautics and Space Administration

I regret that the subject that you have asked me to speak on today is not a sexy one but rather prosaic if not outrightly dull.

While undeniably important, security classification matters do not titillate one's imagination or inspire lightheartedness.

Whereas there is usually something good as well as bad, pleasant as well as unpleasant, about every endeavor, there seems little that is positive about interagency classification matters except need itself. In this field there are no kudos for success, but great is the damnation for failure, and the likelihood of failure is ever present.

To be absolutely perfect in the matter of classification is to just break even.

People in the security business know what Alice meant when she said "it takes all the running you can do to stay in the same place."

Now there are a number of reasons for starting my remarks to you on this pessimistic note.

The first is, the subject justifies it. Classification is an especially dull subject at a time when the whole world is elated by the exploits of Neil Armstrong, Buz Aldrin, and Michael Collins. In the past few days we have witnessed a series of events that have been made even more remarkable by the lack of security classification of any kind, and by the nation's boldness in showing them live, as they occurred, to the entire Western world.

My second reason for this dark approach is that every glimmer of humor or lightheartedness, however faint it may be, that I am able to inject will be doubly welcomed in contrast to the hard, cold facts and debatable opinions that I am about to offer about interagency classification.

You know from long experience that classification problems begin when the *second person* becomes involved in a matter that requires protection. And the complexities multiply at least with the square if not the cube of the number of people and agencies that subsequently become involved.

Now the complexities inherent in this business are further multiplied for those persons who are engaged in classification matters in an organization devoted to science, engineering, and technology – where basic and applied research is conducted – and where new knowledge and new competence are applied toward the solution of important problems, or for provision of the material things needed and wanted by mankind.

These are the areas in which NASA becomes involved, and the areas toward which I want to direct your attention for the next few minutes.

The basis for classification stems from man's needs.

Man's needs are multiple and di-

verse in character.

Security from physical harm by an enemy is one very important human need.

A full measure of the material things required for life is another.

In a democracy such as ours, an informed public is an essential ingredient of good government.

In addition, the American public demands that it know what goes on in government. The average man dislikes secretiveness and is often suspicious of motives which prompt security classification.

To get my presentation in hand, I want to limit myself to identifying *only* a few aspects of Classification Management that arise from the fact that measures required to protect this country and its citizens from military attack depend upon much the same technology that is required to provide the necessities of life in the abundance we want and are accustomed to enjoying. Unfortunately, there is not one unique technology that applies singularly to national security, and other technologies that apply to non-military needs. Science and technology generally apply in varying degrees to both.

Howard Maines, and the others of us in the Classification Management business at NASA, are faced with the requirement of ensuring on the one hand that new and emerging technology can be applied without constraint to the Nation's nonmilitary needs, and on the other hand, that the applications of this same technology toward meeting the Nation's security needs are not disclosed.

But note that we undertake to achieve needed security by protecting the application of technology — not by the classification of technology itself.

Limiting dissemination of knowledge of new scientific discoveries through classification is abhorent to scientists and virtually impossible of successful accomplishment.

It *is* possible, however, to restrict knowledge of new technology — for a while, at least — if the need to do so is recognized early and if the extensive measures required to constrain dissemination are taken promptly and are rigidly enforced.

The technology by which radioactive materials could be extracted and concentrated into critical mass and therefore converted into weapons of great power is perhaps the most often used illustration of successful classification of technology. But the degree of success achieved in this endeavor was not nearly as great as originally hoped for and is still a subject for debate. I certainly have no desire to debate the matter here but would like to speak briefly on some of the "ifs" that are important parts of my assertion that it is possible to constrain dissemination of new technological information for a period of time.

The first "if" is related to the timeliness with which the need to classify is recognized.

The need to classify technology associated with nuclear weapon development was recognized long before initial developments were undertaken. Constraints could therefore be estab-

lished at the very beginning of the program.

Additionally, the nature of the endeavor differed materially from normal industrial pursuits. Engineers and technicians were fully engaged in wartime endeavors of a different character. In addition, research facilities were unique and costly. There was relatively little likelihood, therefore, that individuals or agencies would initiate technological projects that would disclose advanced competence.

Now contrast these conditions and circumstances with those that existed in 1967-68 when it was determined that constraining certain technology pertaining to lasers was important to national security.

The practicability of amplifying light through stimulated emission of radiation had been demonstrated some six to seven years earlier. Man's imagination had been captured. Practical applications were increasingly identified and often demonstrated.

Spectacular progress in increasing the power output of lasers had already been made in Europe and in the USSR — as well as here at home.

Large numbers of highly competent engineers and technicians in nongovernment laboratories were busily striving to advance laser technology. Constraining their activities or information about any activities other than those over which the government had control was virtually impossible.

Normally, we can control dissemination of information about *only* those technological developments over which the government has control. Even these constraining measures may prove futile, for at any time the technology we are trying to protect might be discovered and disclosed by unconstrained engineers in nongovernment agencies at home or abroad. In addition to suffering the stigma of failing, we will have possibly paid a price for constraining distribution of the knowledge for a period of time for new technology, like new science, is normally built on foundations of accomplishment laid down earlier and made known by the successful engineers to their peers.

In summary, the point I want to make here is that conditions and circumstances existing at the time the possibility and potential of nuclear weapons first impacted upon the President and others in authority made it possible to achieve some degree of success in classifying technology.

Different conditions and circumstances prevailed when the potential significance of lasers was first appreciated. We therefore had a different problem and will reap different results.

Now, let me make another point with respect to imposing classification. That point is: We always lose something when we impose constraints.

Don't do it unless you know — and can readily demonstrate to a critical audience — that doing so will achieve positive results that will outweigh the foreseeable negative consequences.

In certain instances, the corollary may be appropriate: that is, we should always classify when the negative impact of disclosure could have deleterious effects far more significant than

the losses that are sustained by classifying. I am sure many of you can recall instances in which we failed to impose effective constraints and paid a great price for our shortcomings.

It is my belief, however, that classification managers should bear the responsibility for achieving unconstrained dissemination of releasable technical information to the same degree that they feel impelled to protect information that requires protection.

The classification manager is not the enemy of the public information officer, or of the personnel charged with achieving wide dissemination of new technical knowledge, but an ally and co-worker. The responsibilities of these three functional officers should not be regarded as conflicting. Instead, the three must appreciate that each bears responsibility for finding an optimum route toward the objectives of each office.

R&D contracting arrangements is one area to which classification managers must give particular attention. Aerospace industries are compartmented for security and other reasons very much like agencies of government are.

Virtually all major firms engage in classified governmental work and do so in limited access facilities. Only certain employees are aware that classified endeavors are being pursued. It requires no great imagination to envisage the problems that might arise if one agency of government, NASA for example, were to undertake to contract openly for R&D work similar to that being performed on a classified basis for another agency of government by the same or by a different contractor. This has happened.

Now one can conceive of circumstances in which such a course of action is determined to be the best way of accomplishing the objectives of both agencies, but it is highly important that there be interfaces between the two government agencies in which certain persons are privy to *all* the work that is being done, and who have responsibilities and authorities necessary to insure that progress is made toward both open and closed objectives, that the government doesn't buy the same technology twice, or otherwise behave unwisely. This is a very delicate matter and one that requires extensive, close interfacing between persons who are alert, imaginative, sensitive, and blessed with good judgment.

Another important point to effective interagency management of classification is that of a common understanding of what objectives are being sought through classification — and of the rules which govern the means we employ.

Common definitions, guidelines, and other well understood criteria for assignment of classification and for the protection of that which is classified is, of course, of great importance. But their importance must not be over estimated. Certainly, rules and regulations must not be allowed to replace thoughtful judgment. This, I think, is particularly important in the classification of R&D endeavors.

R&D is inherently new and different. Often quite different. Criteria created for known conditions and circumstances may not be applicable to

new and different conditions and circumstances. How many people, for example, would recognize the need to classify information on certain mirrors or on how to construct them, or—how many bachelors would anticipate the constraints to be imposed upon him by a wife after marriage? And consider how unwise a new husband would be if he based his behavior pattern after marriage on criteria that was suitable for his bachelor days.

Criteria must be regarded as an important *aid* to judgment, but not a substitute for it.

Decisions as to withholding or releasing information must be made in light of all the known factors bearing upon the matter. Published criteria is a highly important factor, but it is not always the overriding factor.

In summary:

No thoughtful person can deny the need to protect information essential to security of the country.

But neither would responsible persons adopt measures that stifle scientific and technological progress, or unduly curtail the flow of information required either to fulfill the nation's non-military needs or to keep the public appropriately informed.

A sensible path between these two extremes must be found.

Finding such a path is the function of managers concerned with classification and security.

Unusually capable men should be charged with finding practicable ways of achieving needed security on the one hand, and permitting the free flow of information on the other.

The security manager must be a broad-gauged individual, well educated, experienced in human affairs, knowledgeable of the objectives, policies, and activities of the organization of which he is a part. He must be keenly sensitive to the relationships between his organization's activities and national goals and policies. He must keep abreast of the events of the times and be alert to their significance in relation to security.

The security manager must enjoy the respect and have close working relationships with top level executives in the agency in which he is employed. These executives must on the one hand give to the classification manager guidance and direction as to objectives being sought, or the information that must be protected. On the other hand, they must be amendable to the classification manager's advise and direction as to constraints that must be adopted and enforced.

Since virtually every aspect of Classification Management involves multiple agencies of government, it is important that security managers be knowledgeable and sympathetic to the objectives and the policies of the other agencies of government with whom their agency must work.

Classification managers are not afforded the luxury of being provincial. They must view their own activities and those of the agency of which they are a part from a national interest point of view. They must appreciate the policies, objectives, and needs of other agencies of government as well as their own, and recognize that their attainment, like the attainment of those of his own agency, are important

in the national interest.

The security manager must, of course, have the ability to work closely, harmoniously, and effectively with other people. People are the key to successful classification. Personal acquaintance, joint endeavors, mutual respect, and personal friendships facilitate harmonious relationships between people. Meetings such as the one that you are holding here at this time go far to promote wider acquaintance and friendship. In my view they are very worthwhile. I am privileged to participate in this one, and I hope the thoughts I have expressed will cause you to think about them, and perhaps accept, reject, or discuss them.

I thank you.

PUBLIC AFFAIRS IN THE DEPARTMENT OF DEFENSE

Jerry W. Friedheim
Deputy Assistant Secretary of Defense (Public Affairs)

I frankly find it very gratifying to learn of the close relationship which has developed between the security-of-information community and our Defense Public Affairs office.

I am informed that it was not always so.

For too many years — because of opposing objectives—the security and intelligence communities, and the public-affairs community, were roughly 180 degrees out of phase.

At least at Defense we believe we are now in more synchronous orbit, if I can use that phrase on this space-conscious day.

Now, let me say a few words about our professional relationship — your business and my business. I'm sure all of you are aware than security-of-information objectives are subject to several attenuating factors.

Complete secrecy, even in the interests of national security, is not possible nor desirable in a free society. Thus, in pursuing our security objectives we must recognize certain factors which impact upon the Defense Department's security-of-information program.

From time to time national security itself, will dictate the release of information which has been classified, in fact sometimes highly classified.

For instance, it might be that there is a requirement to make our deterrence more credible.

Another consideration is the requirement to justify the budget. To enable the Congress to perform its legislative mission, it must be furnished full and complete information, both classified and unclassified, concerning all aspects of the current and future activities of the Department of Defense.

Generally this is provided through the testimony of a large number of senior Defense Department officials, both civilian and military, before Congressional committees. This is as it should and must be.

A third factor which must concern us in our endeavor to deny information of value to an enemy is our lack of ability to protect some of this information. Our free society and free press make it impossible and undesirable to protect many of the same types of information which the Soviet system withholds from us.

This leads me to the role of my office. Within the Department of Defense the Office of the Assistant Secretary for Public Affairs acts as the DOD agency here at the seat of government for the release of official information through the public information media.

And, on March 4, Secretary Laird issued a memorandum which set forth four public-information principles that guide us. He said:

"1. Our first concern must be the security of the United States and the safety of our armed forces. Therefore, information which would adversely affect the security of our country or endanger its men should not be disclosed.

"2. The provisions of the Freedom of Information Act will be supported in both letter and spirit.

"3. No information will be classified solely because disclosure might result in criticism of the Department of Defense.

"4. . . . . the sole purpose of (public affairs) planning and coordination will be to expedite the flow of information to the public. Propaganda has no place in DOD public information programs."

I want to assure you that these principles are clearly understood by our Public Affairs people to be unequivocal statements of policy. They form the foundation for our efforts to clearly identify that information which must be withheld in the national-security interest and our determination to make the remainder available to the public.

As you probably know, Mr. Gilbert Fitzhugh, Chairman of the Board of Metropolitan Life, was recently named by the President to be chairman of a blue ribbon panel to study the Department of Defense. A newsman asked him if he was approaching this task with any preconceived ideas. Mr. Fitzhugh replied that he had read in the papers that there were quite a few things wrong with the Department of Defense and he had often thought "somebody ought to look into it. Well, now," said Mr. Fitzhugh, "it looks like it will be me."

Well, I am in a somewhat similar position. Both as a reporter and as a Congressional staff member, I had felt there was room for improvement in the release of information to the public by DOD. Now it's up to me to help our Assistant Secretary, Dan Henkin, improve the operation.

One of our continuing objectives is to insure that we do not withhold information unnecessarily.

In that regard, we have, as you know, a Security Review Directorate in Public Affairs headed by Charles Hinkle who has been in this kind of business in the Pentagon since the beginning of time.

The function of Colonel Hinkle's Directorate is to insure that we provide maximum disclosure of information to the public consistent with national security interests. As I have tried to make clear, it's not especially easy to make these national security

determinations.

In fact, it may seem contradictory on first glance to find such a security review function conducted under the Office of the Assistant Secretary for Public Affairs. I'm responsible for the Directorate for Security Review—and I'm also responsible for the Directorate for Defense Information. I have therefore the job both of getting the information out, and of preventing disclosure of classified information.

We feel in Defense Public Affairs, however, that these dual responsibilities—protecting and releasing information—logically belong together.

There must be one place where both security and public information requirements are finally reconciled, and the fact that the Directorate for Security Review operates under the jurisdiction of public affairs is highly significant, because that means the main thrust is in the direction of disclosing all information which can safely be released.

The new administration has been in office slightly over six months now and we have been reviewing our policies and procedures in some detail.

Although our public affairs studies are not yet complete we have taken some steps designed to provide a more open flow of defense information to the public.

Examples are our daily 10:30 meeting with the Pentagon correspondents, normally conducted by Secretary Henkin or me; and our strong emphasis on providing to the Congress and the American people the maximum amount of unclassified information on the fiscal year 1970 budget.

There has been considerable budget data which has not been publicly disclosed in the past. After careful review, we have been able to disclose a great many of these important facts to the public.

I would like to describe for you some of our normal day-to-day operations. Unfortunately, there are no really routine days for us, so let me just give you a few examples of what we have done recently to make information available to the public rapidly and in depth.

About midnight April 15, a United States Navy EC-121 was shot down by the North Koreans in the Sea of Japan. It had been on a classified mission, yet the initial DOD news release was made by the Directorate for Defense Information at 5 a.m. By the end of that first day three detailed situation reports had been released along with seven additional releases containing the names of crew members. Radio and TV news media were notified, and Secretary Henkin read a Defense Department statement for cameras and radio.

The story continued until April 25 and ended with the release of a comprehensive fact sheet on the incident compiled by The Joint Chiefs of Staff. During this period 25 news releases and 13 filming sessions occurred. Still and motion picture materials were made available both here and in Japan.

As a result of this effort, the American people had full knowledge of the incident at all times.

This did not just happen. It required intimate coordination and cooperation between the Directorate for Security Review and Directorate for Defense Information, between DOD and the State Department; it involved

the Joint Chiefs of Staff and Congressional committees — yet at all times the story was told, while security was protected.

In May we had a problem of a different sort — the disposal of obsolescent chemical munitions by the Army. Our efforts to provide information on this project are not yet ended, of course, because the munitions have not yet been disposed of.

In May, however, it was necessary to begin providing a considerable amount of information on chemical munitions matters. Since then there has been a detailed press briefing, detailed unclassified Congressional testimony by Army witnesses and ten news releases. We expect there will be more yet. It has been the most substantial public discussion of chemical warfare in our nation's history.

Details of a chemical mishap on Okinawa have just this week been fully aired; yet essential security has been preserved.

On June 2, we learned that one of our destroyers, the USS Frank E. Evans, had been cut in two in a collision with the Australian carrier Melbourne during SEATO exercises in the South China Sea. News releases were made both by our office and by the Commander in Chief, Pacific Fleet. Our first release was at 6:50 p.m., June 2, and within a short time the Naval Commander at Hawaii was given authority to release all information concerning the collision.

Despite the fact that the actual source of news was then in Hawaii, we continued to make information available to members of the Pentagon press corps, and during that first night provided them with details and background information on 17 different occasions. This assistance continued throughout succeeding days.

Then, of course, the ABM debate has been long underway.

Secretary Laird has more completely and fully discussed the details of Soviet missile strength than ever before.

Senators on both sides have requested and received clearances to lay all sorts of previously classified facts on the line.

And the debate goes on.

Now, not everyone will agree with the specifics of what we have done in these cases. But the point I want to make is a rational decision was made in each of these cases I have described.

In the EC-121 case, for instance, we cleared release of the plane's flight route, but we protected the detailed operations of Task Force 71.

In the case of chemicals, we cleared plans that were underway to remove chemical munitions from Okinawa, but protected the exact nature and size of our deterrent stocks.

In the sea collision we laid out the disaster details and ships involved, while guarding SEATO contingency plans.

In the ABM debate we disclosed Soviet capabilities, while protecting intelligence sources.

In each of these instances, we went through the same procedure. We considered the need to protect information which affected national security within the meaning of Executive Order 10-501. We considered our responsibilities to keep the public informed, as required by the policy laid down by Secretary Laird, and in keep-

ing with the Freedom of Information Act.

Once we determined that we could release information on these matters, we used all our resources to release it rapidly and as much detail as possible.

That's the kind of work we do and I want all of you to know that the complex nature of the problem with which you deal in the security classification community is thoroughly appreciated by those of us in Defense public affairs.

We think it's worth all the trouble because in the last analysis our society depends on the existence of an enlightened public, a public that is in possession of the facts and that thus can make reasoned judgments on national affairs.

There are no easy answers, no final judgments, and no room for error, and we share these hazards with you.